UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

EUCLIDEAN, CONFORMAL, AND HYPERBOLIC GEOMETRY OVER CLASSICAL, FINITE AND OTHER FIELDS

A Dissertation

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

degree of

Doctor of Philosophy

By

CHARLOTTE KAYE SIMMONS

Norman, Oklahoma

1998

EUCLIDEAN, CONFORMAL AND HYPERBOLIC GEOMETRY OVER CLASSICAL, FINITE AND OTHER FIELDS

A Dissertation APPROVED FOR THE DEPARTMENT OF MATHEMATICS

BY

Murad Özaydin

Leonard R. Rubin

Kevin C. Grasse

Ara Basmajian

Ronald Kantowski

IN LOVING MEMORY OF MY FATHER

CHARLES R. SIMMONS

ACKNOWLEDGEMENTS

Words are inadequate to express my deep gratitude and appreciation to my advisor Dr. Murad Özaydın for being a constant source of encouragement, patience, wisdom and guidance thoughout my graduate studies. Thank you for all you have taught me and for being both the best advisor I could ever have asked for and a true friend.

I would like to thank Dr. Ara Basmajian, Dr. Kevin Grasse, Dr. Leonard Rubin and Dr. Ronald Kantowski for serving on my committee and for all their contributions to my education. A special thanks to Dr. Basmajian who went above and beyond the call of duty by meeting with me several hours when I was preparing for generals and again later when my advisor was on sebbatical.

I would like to thank Dr. Stuart Anderson who is the reason I decided to pursue a graduate degree in the first place and the reason I kept going on several occasions when times were tough. You have been a source of encouragement and a cheerful supporter all along the way. Thank you for believing in me.

Finally, I wish to dedicate this thesis to my father Charles (who passed away just before it was completed), to my mother Ovella and to my sister Ruby. Without their love, support, encouragement and prayers throughout the years, I would never have made it this far.

TABLE OF CONTENTS

INTRODUCTION

Let $\mathbb{E}$ be a quadratic Galois extension of $\mathbb{F}$ where the characteristic of $\mathbb{F}$ is not two. We develop a hyperbolic geometry in this general set-up where $\mathbb{H} = \mathbb{E} - \mathbb{F}$ is the hyperbolic plane model. When $\mathbb{F} = \mathbb{R}$ and $\mathbb{E} = \mathbb{C}$, we get the classical case except that our hyperbolic plane is really a union of the upper and lower half planes. It is necessary to define $\mathbb{H}$ in this way because $PSL_2(\mathbb{F})$ acts transitively on $\mathbb{H}$ for many fields. In particular, this is true when $\mathbb{F}$ is finite, a case of primary importance to us. Though the classical case and the finite case are of the most interest to us, working in the more general set-up does prove to be advantageous. For instance, we get some applications in number theory to diophantine equations when $\mathbb{F}$ is the field of rational numbers.

This work was motivated by our desire to develop a deeper understanding of the group $PSL_2(q)$ (the projective linear group of 2×2 matrices with entries in the field $\mathbb{F}_q$ with q elements where $q = p^n$ and p is an odd prime). In an earlier work [OST], we solved the Spherical Hurwitz Problem for $PSL_2(q)$ (the determination and classification of Riemann surfaces that admit orientation preserving symmetries isomorphic to $PSL_2(q)$ with quotient the sphere) where q is a prime power larger than eleven and q is odd. The Spherical Hurwitz Problem is equivalent to the Inverse Galois Problem for the function field $\mathbb{C}(t)$ (the determination and classification of Galois extensions of $\mathbb{C}(t)$ with Galois group isomorphic to $PSL_2(q)$). The Inverse Galois Problem is open for the field of rational numbers and the group $PSL_2(p)$ for infinitely many primes p. Our viewpoint is that a group is what a group does–sort of an inverted Klein point of view. That is, one should understand a group ($PSL_2(q)$ for instance) by realizing it as the group of allowable transformations of a geometry and then studying that geometry to gain insights about the group.

The group of allowable transformations of our hyperbolic geometry is $PGL_2(\mathbb{F})$, which contains $PSL_2(\mathbb{F})$ as a subgroup (of index two in the finite case). The underlying space of our Euclidean geometry is $\mathbb{E}$. The $Ax + B$ group (which is the stabilizer of infinity in $PGL_2(\mathbb{E})$) acts as similarities on $\mathbb{E}$. The projective space $\mathbb{E} \cup \{\infty\}$ and the group $PGL_2(\mathbb{E})$ give a conformal geometry. $PGL_2(\mathbb{E})$ acts on $\mathbb{E} \cup \{\infty\}$ taking the set of lines and circles into itself and preserving "dengles".

The need for our notion of the "dengle" or double exponential angle between two lines stems from the fact that our fields are not necessarily ordered. Consequently, there are no "rays" in our set-up making it impossible to define the angle between two lines. There are, in fact, two angles, θ and $\theta - \pi$, between two given lines. We get around this problem by defining an analog of $e^{2i\theta}$ $(= e^{2i(\theta-\pi)})$ from the classical case.

In general, much of the classical theory holds true in our set-up. However, we do have unexpected peculiarities. For instance, a line may pass through the center of a circle without intersecting the circle. In fact, when $\mathbb{F}$ is finite, exactly half of the lines passing through the center of a circle will intersect it. Therefore, while most of our results are motivated by our geometric intuition from the classical case, the proofs are algebraic. We rely heavily on group theory and, in particular, on group actions.

Our analog of hyperbolic distance takes values in $\mathbb{F}$ and is preserved by the group $PGL_2(\mathbb{F})$. When $\mathbb{F} = \mathbb{R}$ and the two points are in the upper half-plane, this analog turns out to be $\sinh^2(\frac{\rho}{2})$ where ρ is the classical hyperbolic distance. While the concept of the "shortest" path between two points makes no sense in our context, we have "geodesics" which are the fixed point sets of hyperbolic reflections. This is also the case classically. Moreover, our geodesics turn out to be vertical lines and circles centered on $\mathbb{F}$ as one would expect. Classically, however, geodesics are orthogonal to $\widehat{\mathbb{F}}$ and are all equivalent under the isometry group $PSL_2(\mathbb{R})$. This is no longer true in this generality. There can be many different equivalence classes of geodesics since not all geodesics intersect $\mathbb{F}$. In the finite case, there are two–those having $q+1$ points and those having $q-1$. We therefore lose the powerful technique of normalizing from the classical set-up. Furthermore, the concepts of "perpendicular" and "orthogonal" are distinct in our geometry. Two geodesics can be orthogonal without intersecting. We reserve the term perpendicular to describe orthogonal geodesics which intersect.

We recently became aware of the work of Audrey Terras and her students. In [T], Terras defines finite hyperbolic space and a hyperbolic distance on the space which agrees with ours up to a scalar. However, we are able to define hyperbolic distance without using a choice of coordinates. She also associates to every distance in $\mathbb{F} - \{0, -1\}$ a graph which is Ramanujan. Ramanujan graphs play a very important role in computer science as they are the best possible expanders amongst graphs of fixed degree. We define a generalization of the Terras graphs which we conjecture are also Ramanujan. The construction of these graphs uses triangle groups and relates to our work on the Spherical Hurwitz Problem. It is an open question whether or not the Terras graphs are all nonisomorphic [T] but we show that there are at least three isomorphism types when $q > 3$.

In Sections 4 and 5 we concentrate on $PSL_2(\mathbb{F})$. In Section 4 we classify the finite subgroups of $PSL_2(\mathbb{F})$ and count the number of subgroups of $PSL_2(q)$. We do not know of any modern reference which does the latter. Both problems were solved by Dickson for $\mathbb{F} = \mathbb{F}_q$ in the early 1900's though our arguments are more geometric than his. In Section 5 we compute the Eichler cohomology of every subgroup of $PSL_2(p)$ as well as some subgroups of $PSL_2(p^n)$.

0. Notation and Preliminaries.

Let $\mathbb{E}$ be a quadratic Galois field extension of $\mathbb{F}$ with $\mathrm{char}(\mathbb{F}) \neq 2$. Let $f(x) = x^2 + \beta$ be an irreducible quadratic in the ring $\mathbb{F}[x]$ of polynomials with coefficients in $\mathbb{F}$. Let $\pm\alpha$ be the roots of $f(x)$ in $\mathbb{E}$. Then

$$\mathbb{E} \cong \mathbb{F}[x]/\langle f(x)\rangle \cong \mathbb{F} \oplus \mathbb{F}\alpha.$$

Thus, any element of $\mathbb{E}$ can be expressed uniquely as $a + b\alpha$ with $a, b \in \mathbb{F}$. We also note that $\beta = -\alpha^2$.

For example, when $\mathbb{F} = \mathbb{R}$ and $\mathbb{E} = \mathbb{C}$, we get the classical case of $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}i$. Another special case that will be of interest to us (referred to hereafter as the finite case) occurs when $\mathbb{F} = \mathbb{F}_q, q = p^n$. Here $\mathbb{E} = \mathbb{F}_{q^2}$.

We define the projective space of dimension one over $\mathbb{F}$, denoted $\mathbb{P}^1_{\mathbb{F}}$, via $\mathbb{P}^1_{\mathbb{F}} = \mathbb{F}^\times I \backslash \mathbb{E}^\times$.

Since any element $[u : v] \in \mathbb{P}^1_{\mathbb{F}}$ can be written uniquely as $[\frac{u}{v} : 1]$ if $v \neq 0$ or $[1 : 0]$ if $v = 0$, $\mathbb{P}^1_{\mathbb{F}}$ can be identified with $\mathbb{F} \cup \{\infty\}$. Analogously, $\mathbb{P}^1_{\mathbb{E}} = \mathbb{E} \cup \{\infty\}$.

Given a field $\mathbb{K}$,

$$GL_2(\mathbb{K}) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mid a, b, c, d \in \mathbb{K}, ad - bc \neq 0 \right\},$$

$$SL_2(\mathbb{K}) := \{ A \in GL_2(\mathbb{K}) \mid det(A) = 1 \}.$$

We will consider the matrix groups

$$PGL_2(\mathbb{K}) := GL_2(\mathbb{K})/\mathbb{K}^\times \mathrm{I} \text{ and } PSL_2(\mathbb{K}) := SL_2(\mathbb{K})/\{\pm \mathrm{I}\}$$

where $\mathbb{K}$ is $\mathbb{E}$ or $\mathbb{F}$.

Given an element $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $GL_2(\mathbb{K})$ (respectively $SL_2(\mathbb{K})$), we will denote its equivalence class in $PGL_2(\mathbb{K})$ (respectively $PSL_2(\mathbb{K})$) via $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

The elements of $PGL_2(\mathbb{K})$ (respectively $PSL_2(\mathbb{K})$) can also be viewed as linear fractional transformations via the obvious identification of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $GL_2(\mathbb{K})$ (respectively $SL_2(\mathbb{K})$) with the transformation $g(z) = \frac{az+b}{cz+d}$. We will use the two formulations of the groups interchangeably throughout.

Viewed as linear fractional transformations, the groups $PGL_2(\mathbb{F})$, $PSL_2(\mathbb{F})$, $PGL_2(\mathbb{E})$, $PSL_2(\mathbb{E})$ all act on $\mathbb{P}^1_{\mathbb{E}}$ in the obvious way. (Equivalently, the action is given by matrix multiplication: $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} au+bv \\ cu+dv \end{bmatrix}$.)

Remark: Given P, Q, R distinct in $\mathbb{P}^1_{\mathbb{E}}$, there is an element h of $PGL_2(\mathbb{E})$ satisfying $h(P) = 0, h(Q) = \infty$, and $h(R) = 1$. If all of the points are in $\mathbb{E}$, then

$$h(z) = \left(\frac{R-Q}{R-P}\right)\left(\frac{z-P}{z-Q}\right).$$

Otherwise,

$$h(z) = \frac{R-Q}{z-Q},\ h(z) = \frac{z-P}{R-P},\ h(z) = \frac{z-P}{z-Q}$$

when P, Q, or R respectively is ∞.

Theorem 0.1. *$PGL_2(\mathbb{E})$ acts triply transitively on $\mathbb{P}^1_{\mathbb{E}}$. The action of $PGL_2(\mathbb{F})$ is transitive on $\mathbb{E} - \mathbb{F}$ and triply transitive on $\mathbb{P}^1_{\mathbb{F}}$.*

Proof: Given $x = a + b\alpha \in \mathbb{E} - \mathbb{F}$, let $g(z) = bz + a$. Then $g \in PGL_2(\mathbb{F})$ and $g(\alpha) = x$. So $PGL_2(\mathbb{F})$ acts transitively on $\mathbb{E} - \mathbb{F}$.

$PGL_2(\mathbb{E})$ acts transitively on $\mathbb{P}^1_{\mathbb{E}}$ by the above Remark. If $P, Q, R \in \mathbb{P}^1_{\mathbb{F}}$ are distinct then the h in the Remark is in $PGL_2(\mathbb{F})$. $\square$

The stabilizer of the set Y in the group G will be denoted G_Y or G_x if $Y = \{x\}$.

An easy computation shows that

$$\begin{aligned} PGL_2(\mathbb{F})_\infty &= \{\, ax+b \mid a \in \mathbb{F}^\times, b \in \mathbb{F} \,\}, \\ PGL_2(\mathbb{F})_\alpha &= \left\{ \frac{az - b\beta}{bz + a} \mid a, b \in \mathbb{F}, a \neq 0 \text{ or } b \neq 0 \right\}. \end{aligned}$$

Consequently, there are exactly two orbits of the action of $PGL_2(\mathbb{F})$ on $\mathbb{P}^1_{\mathbb{E}}$, namely $\mathbb{F} \cup \{\infty\}$ and $\mathbb{E} - \mathbb{F}$.

Theorem 0.2. *$PSL_2(\mathbb{E})$ acts doubly transitively on $\mathbb{P}^1_{\mathbb{E}}$ and $PSL_2(\mathbb{F})$ acts doubly transtively on $\mathbb{P}^1_{\mathbb{F}}$.*

Proof: Given $P, Q \in \mathbb{P}^1_{\mathbb{E}}$, $g(z) = (\frac{1}{P-Q})(\frac{z-P}{z-Q}) \in PSL_2(\mathbb{E})$ and $g(P) = 0, g(Q) = \infty$. If $P, Q \in \mathbb{P}^1_{\mathbb{F}}$, then $g \in PSL_2(\mathbb{F})$. $\square$

Notation:

i) $\mathbb{K}^\times := \{\, k \in \mathbb{K} \mid k \neq 0 \,\}$.

ii) $\mathbb{K}_+ := \{\, k^2 \mid k \in K^\times \,\}$.

Note that $\mid \ker(\square) \mid = 2$ where $\square : \mathbb{K}^\times \to \mathbb{K}_+$ is the squaring map. In particular, $\mathbb{K}_+$ has index two in $\mathbb{K}^\times$ when $\mathbb{K}$ is finite.

We can also write

$$PSL_2(\mathbb{F}) = \left\{ \frac{ax+b}{cx+d} \mid a, b, c, d \in \mathbb{F},\ ad - bc \in F_+ \right\}$$

since

$$\frac{ax+b}{cx+d} = \frac{\frac{a}{r}x + \frac{b}{r}}{\frac{c}{r}x + \frac{d}{r}} \text{ and } \det(\begin{pmatrix} \frac{a}{r} & \frac{b}{r} \\ \frac{c}{r} & \frac{d}{r} \end{pmatrix}) = 1 \text{ when } ad - bc = r^2.$$

Thus, we have

$$\begin{aligned} PSL_2(\mathbb{F})_\infty &= \{ \ ax + b \mid a \in \mathbb{F}_+, b \in \mathbb{F} \ \}, \\ PSL_2(\mathbb{F})_\alpha &= \left\{ \ \frac{az - b\beta}{bz + a} \mid a, b \in \mathbb{F}, a^2 - b^2\beta \in \mathbb{F}_+ \ \right\}. \end{aligned}$$

The following theorem, together with Theorem 0.2, thus says that there are also exactly two orbits of the action of $PSL_2(\mathbb{F})$ on $\mathbb{P}^1_{\mathbb{E}}$ when $\mathbb{F}$ is finite.

Theorem 0.3. *When $\mathbb{F}$ is finite, $PSL_2(\mathbb{F})$ acts transitively on $\mathbb{E} - \mathbb{F}$.*

Proof: Let $a + b\alpha \in \mathbb{E} - \mathbb{F}$. If $b \in \mathbb{F}_+$, then $g(z) = bz + a \in PSL_2(\mathbb{F})$ and $g(\alpha) = b\alpha + a$. If $b \in \mathbb{F}^\times - \mathbb{F}_+$, then $b = c\beta^{-1}$ for some $c \in \mathbb{F}_+$ (since $\mathbb{F}^x/\mathbb{F}_+$ has degree two, $b\mathbb{F}_+ = \beta\mathbb{F}_+$). Then $h(z) = \frac{-c}{z} + a \in PSL_2(\mathbb{F})$ and $h(\alpha) = a + b\alpha$. $\square$

Lemma 0.4.

$PGL_2(\mathbb{F})$ acts transitively on $(\mathbb{E} - \mathbb{F}) \times \widehat{\mathbb{F}} = \{ \ (w, x) \mid w \in \mathbb{E} - \mathbb{F}, x \in \widehat{\mathbb{F}} \ \}$.

Proof: Let $w = a + b\alpha \in \mathbb{E} - \mathbb{F}$, $x \in \widehat{\mathbb{F}}$. Then $g(\alpha) = w$ where $g(z) = bz + a$. Consequently, $g^{-1}(w) = \alpha$. Let $y = g^{-1}(x)$. Then $y \in \widehat{\mathbb{F}}$ since g (and hence g^{-1}) preserves $\widehat{\mathbb{F}}$.

If $y = \infty$, then $g^{-1}(w) = \alpha$ and $g^{-1}(\infty) = \infty$. If $y \neq \infty$, then $k(\infty) = y$ where $k(z) = \dfrac{yz + \alpha^2}{z + y} \in PGL_2(\mathbb{F})_\alpha$. Consequently, $k^{-1} \circ g^{-1}(w) = \alpha$ and $k^{-1} \circ g^{-1}(x) = k^{-1}(y) = \infty$. Hence, we can always find an element of $PGL_2(\mathbb{F})$ taking the pair (w, x) to the pair (α, ∞). $\square$

We define the **conjugate** of an element $\lambda = a + b\alpha$ in $\mathbb{E}$ to be $a - b\alpha$, denoted $\overline{\lambda}$.

Conjugation is a field automorphism of $\mathbb{E}$ fixing $\mathbb{F}$.

Given $1 \neq f(x) = \frac{ax+b}{cx+d} \in PGL_2(\mathbb{F})$, we consider the fixed points of f.

If $c \neq 0$, then

$$\begin{aligned} f(x) = x \quad &\Longleftrightarrow \quad cx^2 - (a-d)x - b = 0 \\ &\Longleftrightarrow \quad x = \frac{(a-d) \pm \sqrt{(a-d)^2 + 4bc}}{2c}. \end{aligned}$$

The discriminant $\Delta = (a-d)^2 + 4bc = (a+d)^2 - 4(ad-bc) = tr^2(f) - 4det(f)$. $\Delta \in \mathbb{F}_+ \implies$ i) f has two fixed points in $\mathbb{P}^1_{\mathbb{F}}$, none in $\mathbb{E} - \mathbb{F}$ $\quad \Delta = 0 \implies$ ii) f has one fixed point in $\mathbb{P}^1_{\mathbb{F}}$, none in $\mathbb{E} - \mathbb{F}$. $\Delta \in \mathbb{F}^\times - \mathbb{F}_+ \implies$ iii) f has no fixed points in $\mathbb{P}^1_{\mathbb{F}}$.

If $\Delta \in \mathbb{E}_+$ in iii), then f has two conjugate fixed points (since they are the roots of an irreducible quadratic). Otherwise, f has no fixed points.

If $c = 0$, then the only fixed point of f is ∞ and we again get result ii).

We define the type of $1 \neq g \in PGL_2(\mathbb{F})$ to be hyperbolic, parabolic or elliptic if g satisfies condition i), ii) or iii) respectively.

In the finite case, $\mathbb{F}^\times \subseteq \mathbb{E}_+$. (Since $q-1$ divides $|\mathbb{E}_+| = q^2 - 1$, there must be a subgroup of $\mathbb{E}_+ \subseteq \mathbb{E}^\times$ of order $q-1$. But the unique such subgroup is $\mathbb{F}^\times$). Consequently, all elliptic elements have two fixed points in $\mathbb{E} - \mathbb{F}$ in the finite case.

Since $PGL_2(\mathbb{F})$ acts doubly transitively on $\mathbb{P}^1_{\mathbb{F}}$ and transitively on $\mathbb{E} - \mathbb{F}$, and the type of an element is invariant under conjugation, we can conjugate a nonidentity element of $PGL_2(\mathbb{F})$ with nonempty fixed point set to have fixed point set $\{0,\infty\}, \{\infty\}$, or $\{\alpha,\overline{\alpha}\}$.

We therefore have the following proposition.

Proposition 0.5. *Every $1 \neq g \in PGL_2(\mathbb{F})$ is one of the following:*

i) *hyperbolic* *iff* $tr^2(g) - 4det(g) \in \mathbb{F}_+$

iff g *is conjugate to* ax *for some* $a \in \mathbb{F}^\times$

ii) *parabolic* *iff* $tr^2(g) = 4$

iff g *is conjugate to* $x+b$, $b \in \mathbb{F}^\times$

iii) *elliptic* *iff* $tr^2(g) - 4det(g) \in \mathbb{F}^\times - \mathbb{F}_+$

(iff g *is conjugate to an element of the form* $\frac{az-b\beta}{bz+a}$, $a, b \in \mathbb{F}$ *if* g *has a fixed point).*

Note that a similar fixed point analysis for $1 \neq g \in PGL_2(\mathbb{E})$ shows that g has at most two fixed points. Consequently, if two nonidentity elements g, h of $PGL_2(\mathbb{E})$ agree on three distinct points, then $g = h$. ($h^{-1} \circ g$ fixes three points.) In view of this fact and Theorem 0.1, we now know that $PGL_2(\mathbb{E}), PGL_2(\mathbb{F})$ act sharply triply transitively on $\mathbb{P}^1_{\mathbb{E}}, \mathbb{P}^1_{\mathbb{F}}$ respectively.

Consider the finite case. Let $PSL_2(q) := PSL_2(F_q)$. Then $|PSL_2(q)| = \frac{q(q+1)(q-1)}{2}$, $|\mathbb{P}^1_{\mathbb{F}}| = q^2+1$, $|F_{q^2} - F_q|$. Since the action of $PSL_2(q)$ is transitive on both $\mathbb{P}^1_{\mathbb{F}}$ and $\mathbb{F}_{q^2} - \mathbb{F}_q$, we have

$$|PSL_2(q)_\infty| = \frac{|PSL_2(q)|}{|\mathbb{P}^1_{\mathbb{F}_q}|} = \frac{q-1}{2} \text{ and } |PSL_2(q)_\alpha| = \frac{|PSL_2(q)|}{|\mathbb{F}_{q^2} - \mathbb{F}_q|} = \frac{q+1}{2}.$$

We thus have the following proposition.

Proposition 0.6. *Every $1 \neq g \in PSL_2(q)$ is one of the following:*

i) *g is hyperbolic*   *iff* $tr^2(g) - 4 \in (\mathbb{F}_q)_+$

iff g *is conjugate to* ax, $a \in (\mathbb{F}_q)_+$

iff $ord(g) | \frac{q-1}{2}$

ii) *g is parabolic*   *iff* $tr^2(g) = 4$

iff g *is conjugate to* $x+b$, $b \in (\mathbb{F}_q)^\times$

iff $ord(g)=p$

iii) *g is elliptic*   *iff* $tr^2(g) - 4 \in (\mathbb{F}_q)^\times - (\mathbb{F}_q)_+$

iff g *is congugate to an element of the form*

$$\frac{az - b\beta}{bz + a}, \; a, b \in \mathbb{F}_q$$

iff $ord(g) | \frac{q+1}{2}$.

We note that the order of an element of $PGL_2(q)$ does not determine its type since an element of order two could be either hyperbolic or elliptic.

The norm map $N : \mathbb{E}^\times \to \mathbb{F}^\times$ is defined by $N(\lambda) = \lambda\overline{\lambda}$. We will say that $\lambda\overline{\lambda}$ is the **norm** of λ.

Of course, this map is not surjective in general (e.g., $\mathbb{F} = \mathbb{R}, \mathbb{E} = \mathbb{C}$), but the following lemma shows that it is in the finite case.

Lemma 0.7. *$N : (\mathbb{F}_{q^2})^\times \to (\mathbb{F}_q)^\times$ is surjective.*

Proof: $\lambda \in \ker(N)$ iff $1 = \lambda\overline{\lambda} = \lambda\overline{\lambda}^q = \lambda^{q+1}$. So $|ker(N)| =$ q+1. Thus,

$$|Im(N)| = \frac{|(\mathbb{F}_{q^2})^\times|}{|ker(N)|} = \frac{q^2-1}{q+1} = q - 1 = |(\mathbb{F}_q)^\times|. \quad \square$$

Note that $\mathrm{Im}(N) \subseteq \mathbb{E}_+$ in this case.

1. Euclidean Geometry.

Throughout this paper, we will assume that $\mathbb{E}$ is a quadratic Galois extension field of $\mathbb{F}$ with char($\mathbb{F}$) $\neq 2$. Then $\mathbb{E} \cong \mathbb{F} \oplus \mathbb{F}\alpha$ where α is a root in $\mathbb{E}$ of the irreducible polyomial $x^2 + \beta \in \mathbb{F}[x]$.

Given $\lambda \in \mathbb{E}$, $\lambda = \frac{\lambda+\overline{\lambda}}{2} + \frac{\lambda-\overline{\lambda}}{2}$ where $\frac{\lambda+\overline{\lambda}}{2} \in \mathbb{F}$.

We call $\lambda = \frac{\lambda+\overline{\lambda}}{2}$ the **real part** of λ and $\frac{\lambda-\overline{\lambda}}{2}$ the **imaginary part** of λ (denoted $\mathrm{Re}(\lambda)$, $\mathrm{Im}(\lambda)$ respectively).

Let $\mathbb{I} = \{\, \lambda - \overline{\lambda} \mid \lambda \in \mathbb{E} - \mathbb{F}^{\times} \} = \{\, \lambda \in \mathbb{E} \mid \overline{\lambda} = -\lambda\}$.

We call $\mathbb{I}$ the **imaginary axis** of $\mathbb{E}$.

Let $\mathbb{S} = \{\, \lambda \in \mathbb{E}^{\times} \mid \lambda\overline{\lambda} = 1\}$ and $\mathbb{T} = \{\, \lambda \in \mathbb{E}^{\times} \mid \lambda\overline{\lambda} = -1\}$.

We call $\mathbb{S}$ the **unit circle** of $\mathbb{E}$ and $\mathbb{T}$ the **unit imaginary circle** of $\mathbb{E}$.

Note that $\mathbb{I}$ and $\mathbb{S}$ are nonempty for any $\mathbb{E}$ but $\mathbb{T}$ may be empty.

We observe the following simple but useful facts.

Facts:

i) $m, n \in \mathbb{I} - \{0\} \implies mn, \frac{m}{n} \in \mathbb{F}$

ii) $\mathbb{F}^{\times}(\mathbb{I} - \{0\}) = \mathbb{I} - \{0\}$

iii) $\mathbb{F} \cap (\mathbb{I} - \{0\}) = \emptyset = \mathbb{I} \cap \mathbb{T}$

iv) $\mathbb{F} \cap \mathbb{S} = \{\pm 1\}$

v)

$$\mathbb{I} \cap \mathbb{S} = \mathbb{F} \cap \mathbb{T} = \begin{cases} \{\pm\sqrt{-1}\}, & \text{if } -1 \in \mathbb{E}_{+} \\ \emptyset, & \text{otherwise.} \end{cases}$$

We consider the **Borel** group $B = \{az\ + b \mid a \in \mathbb{E}^\times, b \in \mathbb{E}\}$, the subgroup of $PGL_2(\mathbb{E})$ fixing ∞. Under the action of B on $\mathbb{E}$, we note that $B_0 = \{\ az \mid a \in \mathbb{E}^\times\} \cong \mathbb{E}^\times$. We also have the following lemma.

Lemma 1.1.

i) $B_{\mathbb{F}} = \{\ az + b \mid a \in \mathbb{F}^\times, b \in \mathbb{F}\}\ \ (= PGL_2(\mathbb{F})_\infty)$

ii) $B_{c\mathbb{S}} = \{\ az \mid a \in \mathbb{S}\}$ *for* $c \in \mathbb{E}^\times$.

Proof: i) Clearly if $a, b, \lambda \in \mathbb{F}$, then $a\lambda + b \in \mathbb{F}$. Conversely, assume $a\lambda + b \in \mathbb{F}\ \forall\ \lambda \in \mathbb{F}$. In particular, $\lambda = 0 \implies b \in \mathbb{F}$ and $\lambda = 1 \implies a + b \in \mathbb{F}$. Thus, $a = (a + b) + (-b) \in \mathbb{F}$.

ii) First assume $c = 1$. If $a, \lambda \in \mathbb{S}$, then $(a\lambda)(\overline{a\lambda}) = (a\overline{a})(\lambda\overline{\lambda}) = 1$. Conversely, assume $a\lambda + b \in \mathbb{S}\ \forall\ \lambda \in \mathbb{S}$. Then $(a\lambda + b)(\overline{a\lambda + b}) = a\overline{a} + \overline{a}b\lambda + a\overline{b}\lambda + b\overline{b} = 1\ \forall\ \lambda \in \mathbb{S}$.

In particular, $\lambda = 1 \implies a\overline{a} + \overline{a}b + a\overline{b} + b\overline{b} = 1, \lambda = -1 \implies a\overline{a} - \overline{a}b - a\overline{b} + b\overline{b} = 1$.

Together these two equations imply that $\overline{a}b = -a\overline{b}$. If $b \neq 0$, then $\overline{a}b \in \mathbb{I} - \{0\}$. Since $a\overline{a} + \overline{a}b\lambda + a\overline{b}\lambda + b\overline{b} = 1 = a\overline{a} + b\overline{b}\ \forall\ \lambda \in \mathbb{S}$, we also have $\overline{a}b\lambda \in \mathbb{I} - \{0\}\ \forall\ \lambda \in \mathbb{S}$. Then by Fact i) above, we have $\frac{\overline{a}b\lambda}{\overline{a}b} = \lambda \in \mathbb{F}\ \forall\ \lambda \in \mathbb{F}$. This is a contradiction since $\mathbb{F} \cap \mathbb{S} = \{\pm 1\}$ and $|\mathbb{S}| > 2$. Thus, $b = 0$ and $B_{\mathbb{S}} = \{\ az \mid a \in \mathbb{S}\}$. Thus, $r(c\mathbb{S}) + t = c\mathbb{S}$ iff $r\mathbb{S} + \frac{t}{c} = \mathbb{S}$ iff $r \in \mathbb{S}$ and $t = 0$. $\square$

Lemma 1.2. *The action of B on $\mathbb{E}$ is sharply doubly transitive.*

Proof: It suffices to show that given $P \neq Q \in \mathbb{E}$, there is a unique element

$g \in B$ with $g(P) = 0, g(Q) = 1$. Such an element $g(z) = az + b$ must satisfy the equations $aP + b = 0, aQ + b = 1$. The unique solution to these equations is $a = \frac{-1}{P-Q}, b = \frac{P}{P-Q}$. $\square$

Definition: L is said to be a **line** in $\mathbb{E}$ iff it is the image of $\mathbb{F}$ under a Borel element. I.e., $L = a\mathbb{F} + b$ for some $a \in \mathbb{E}^\times, b \in \mathbb{E}$.

By definition B acts transitively on all lines in $\mathbb{E}$ and we therefore have

$$\frac{|B|}{|B_\mathbb{F}|} = \frac{(q^2-1)q^2}{(q-1)q} = q(q+1)$$

distinct lines in $\mathbb{E}$ in the finite case. Moreover, $|a\mathbb{F} + b| = |\mathbb{F}| = q$. Lemma 1.2 says that any two distinct points in $\mathbb{E}$ determine a unique line. We will often use the notation PQ for the line passing through the distinct points P and Q.

Proposition 1.3. *The following are equivalent descriptions of the line L through $P \neq Q$ in $\mathbb{E}$.*

i) $L = g\mathbb{F}$ *where* $g \in B, g(0) = P, g(1) = Q$

ii) $L = (Q-P)\mathbb{F} + P$

iii) $L = \{ \lambda P + \mu Q \mid \lambda, \mu \in \mathbb{F}, \lambda + \mu = 1\}$.

Proof: Since the unique element of B taking 0 to P and 1 to Q is $g(z) = (Q-P)z + P$, clearly (i) $\Leftrightarrow$ (ii). If $\lambda, \mu \in \mathbb{F}$ with $\lambda + \mu = 1$, then $\lambda P + \mu Q = (1-\mu)P + \mu Q = (Q-P)\mu + P$.

Conversely, if $t \in \mathbb{F}$ then $(Q-P)t + P = (1-t)P + tQ$. Thus, (ii) $\Leftrightarrow$ (iii). $\square$

Definition: L and M are **parallel** (denoted $L \parallel M$) iff $L \cap M = \emptyset$ or $L = M$.

Remark: Since two points determine a line, any two lines are either parallel or intersect in exactly one point.

Lemma 1.4. *Let $L = a\mathbb{F} + b$. The following are equivalent.*

i) $\mathbb{F} \parallel L$

ii) $L = \mathbb{F} + b$

iii) $Q - P \in \mathbb{F} \; \forall \; P, Q \in L$.

Proof: (i) $\Leftrightarrow$ (ii): If $\mathbb{F} = L$, then clearly (ii) holds. Assume $\mathbb{F} \cap L = \emptyset$. Then $\overline{at+b} \neq at + b \; \forall \; t \in \mathbb{F}$. Thus, $(a - \overline{a})t \neq \overline{b} - b \; \forall \; t \in \mathbb{F}$. If $a \notin \mathbb{F}$, then we have that $\frac{\overline{b}-b}{a-\overline{a}} \notin \mathbb{F}$. This is a contradiction to Fact (i) since $\overline{b} - b, a - \overline{a} \in \mathrm{I}$. Thus, $a \in \mathbb{F}$ and $L = \mathbb{F} + b$.

(ii) $\implies$ (i): If $\exists \; t \in \mathbb{F} \cap L$, then $t = r + b$ for some $r \in \mathbb{F}$. Thus, $b = (r + b) - r \in \mathbb{F}$. So either $L = \mathbb{F}$ or $\mathbb{F} \cap L = \emptyset$.

(ii) $\Leftrightarrow$ (iii): If $L = \mathbb{F} + b$, then $P, Q \in L \implies P = r + b, Q = t + b$ for some $r, t \in \mathbb{F}$. Thus, $Q - P = t - b \in \mathbb{F}$. Conversely, since $0, 1 \in \mathbb{F}$ and $L = a\mathbb{F} + b$, we know $b, a + b \in L$. Then $a = (a + b) - b \in \mathbb{F}$. $\square$

Remark: It is clear from Lemma 1.4(ii) that the parabolic subgroup $P = \{ \, z + \alpha \mid \alpha \in \mathbb{E}\}$ of B acts transitively on all lines parallel to $\mathbb{F}$. (The element $g(z) = z + (\gamma - \beta)$ takes $\mathbb{F} + \beta$ to $\mathbb{F} + \gamma$.) Thus, in the finite case there are $\frac{|P|}{|stab(\mathbb{F}_q)|} = \frac{q^2}{q} = q$ lines parallel to $\mathbb{F}$. Since any line $L = g\mathbb{F}_q$ for some $g \in B$ and B preserves parallel lines, there are therefore q lines parallel to any given line.

Lemma 1.5. *Let L be a line. If $L \cap \mathbb{F} = \{0\}$, then $L = a\mathbb{F}, a \in \mathbb{E} - \mathbb{F}$. In particular, $\mathbb{I} = a\mathbb{F}$ where $a \in \mathbb{I} - \{0\}$.*

Proof: Since $L \cap \mathbb{F} = \{0\}$, $\exists\, Q \in L - \mathbb{F}$. Then $L = (Q-0)\mathbb{F} + 0 = Q\mathbb{F}$ where $Q \in \mathbb{E} - \mathbb{F}$. If $L = Q\mathbb{F} = \mathbb{I}$, then in particular $Q = Q(1) \in \mathbb{I} - \{0\}$. $\square$

Remarks: i) In fact, since $\mathbb{F}^{\times}(\mathbb{I} - \{0\}) = \mathbb{I} - \{0\}$, $\mathbb{I} = a\mathbb{F}\ \forall\ a \in \mathbb{I} - \{0\}$.

ii) By Lemma 1.5, the hyperbolic subgroup $H = \{\ az \mid a \in E^{\times}\}$ of B acts transitively on all lines through 0. In the finite case, there are $\frac{|\mathbb{E}^{\times}|}{q-1} = q+1$ distinct lines through 0 (since $|L - \{0\}| = q - 1\ \forall$ line L).

Lemma 1.6.

i) *B preserves ratios of the form $\dfrac{A-B}{P-Q}$ where $A \neq B, P \neq Q$ are points in $\mathbb{E}$.*

ii) *If $A \neq B, C \neq D$ lie on a line L and $P \neq Q, R \neq T$ lie on a line M, then $\left(\dfrac{\overline{A}-\overline{B}}{A-B}\right)\left(\dfrac{P-Q}{\overline{P}-\overline{Q}}\right) = \left(\dfrac{\overline{C}-\overline{D}}{C-D}\right)\left(\dfrac{R-T}{\overline{R}-\overline{T}}\right)$.*

Proof: i) Given $g(z) = az + b \in B$,

$$\frac{g(A)-g(B)}{g(P)-g(Q)} = \frac{(aA+b)-(aB+b)}{(aP+b)-(aQ+b)} = \frac{a(A-B)}{a(P-Q)} = \frac{A-B}{P-Q}$$

since $a \in \mathbb{E}^{\times}$.

ii) Since B acts transitively on lines and preserves ratios by i), WMA $L = \mathbb{F}$. Then $A, B, C, D \in \mathbb{F} \implies \frac{\overline{A-B}}{A-B} = 1 = \frac{\overline{C-D}}{C-D}$. It thus suffices to show that $\frac{P-Q}{\overline{P-Q}} = \frac{R-T}{\overline{R-T}}$.

If $\mathbb{F} \parallel M$, then $P-Q, R-T \in \mathbb{F}$ by Lemma 1.4(iii). Therefore, $\frac{P-Q}{\overline{P-Q}} = 1 = \frac{R-T}{\overline{R-T}}$. Otherwise, $|\mathbb{F} \cap M| = 1$. Using i) again, WMA $\mathbb{F} \cap M = \{0\}$. Then

$M = a\mathbb{F}, a \in \mathbb{E} - \mathbb{F}$ by Lemma 1.5. In this case, $R = ar, T = at$ where $r, t \in \mathbb{F}$. Thus,

$$\frac{R-T}{\overline{R}-\overline{T}} = \frac{ar-at}{\overline{a}r-\overline{a}t} = \frac{a(r-t)}{\overline{a}(r-t)} = \frac{a}{\overline{a}}.$$

Similarly, $\dfrac{P-Q}{\overline{P}-\overline{Q}} = \dfrac{a}{\overline{a}}$. $\square$

Definition: Let L, M be lines with $A \neq B \in L, P \neq Q \in M$. The **dengle from** L **to** M is $\left(\dfrac{P-Q}{A-B}\right)\left(\dfrac{\overline{A}-\overline{B}}{\overline{P}-\overline{Q}}\right) \in \mathbb{S}$ and is denoted den(L,M).

Lemma 1.6 says that the dengle is well-defined and is preserved under elements of B.

Proposition 1.7. *Let $A \neq B \in L, P \neq Q \in M$ where L, M are lines. The following are equivalent:*

i) $L \parallel M$

ii) $\dfrac{P-Q}{A-B} \in \mathbb{F}^\times$

iii) *den*$(L, M) = 1$ $(=$ *den*$(M, L))$

iv) $(A-B)(\overline{P-Q}) \in \mathbb{F}^\times$.

Proof:

$$\frac{P-Q}{A-B} \in \mathbb{F}^\times \iff \frac{P-Q}{A-B} = \frac{\overline{P}-\overline{Q}}{\overline{A}-\overline{B}} \iff (\frac{P-Q}{A-B})(\frac{\overline{A}-\overline{B}}{\overline{P}-\overline{Q}}) = 1$$

$$\iff (P-Q)(\overline{A-B}) = (A-B)(\overline{P-Q})$$

$$\iff (A-B)(\overline{P-Q}) \in \mathbb{F}^\times.$$

Thus, (ii) $\Leftrightarrow$ (iii) $\Leftrightarrow$ (iv).

(i) $\iff$ (ii): Since B preserves parallel lines and ratios, WMA $L = \mathbb{F}$. Then $A - B \in \mathbb{F}$ since $A, B \in L = \mathbb{F}$. Thus, $\frac{P-Q}{A-B} \in \mathbb{F}^\times$ iff $P - Q \in \mathbb{F}^\times$ iff $\mathbb{F} \parallel M$ by Lemma 1.4(iii). $\square$

It is clear from Proposition 1.7 that "$\|$ "is an equivalence relation.

We can now show that lines also have a parametric form.

Lemma 1.8. *The line L through $P \neq Q$ is given by*

$$\{z \in \mathbb{E} \mid (z-P)(\overline{z-Q}) = (\overline{z-P})(z-Q)\}.$$

Proof: By Proposition 1.3, $L = \{\ \lambda P + \mu Q \mid \lambda, \mu \in \mathbb{F}, \lambda + \mu = 1\}$. If $\lambda, \mu \in \mathbb{F}$ with $\lambda + \mu = 1$, then

$$\lambda P + \mu Q - P = (1-\mu)P + \mu Q - P = \mu(Q-P),$$

$$\overline{\lambda P + \mu Q - Q} = \lambda(\overline{P-Q}).$$

Thus,

$$\begin{aligned}(\lambda P + \mu Q - P)(\overline{\lambda P + \mu Q - Q}) &= \lambda\mu(\overline{P-Q})(Q-P)\\ &= \lambda\mu(P-Q)(\overline{Q-P})\\ &= (\overline{\lambda P + \mu Q - P})(\lambda P + \mu Q - Q).\end{aligned}$$

Conversely, assume $(z-P)(\overline{z-Q}) = (\overline{z-P})(z-Q)$. Now $z = \lambda P + \mu Q$ where $\mu = \frac{z-P}{Q-P}, \lambda = 1-\mu$. It suffices to check that $\mu \in \mathbb{F}$. By Proposition 1.7(iv), the line L through z and P is parallel to the line M through z and Q. Since $\{P, Q\} \subseteq L \cap M$, $L = M$. Since $\{x, P, Q\} \subseteq L = M$, Proposition 1.7(ii) gives that $\mu = \frac{z-P}{Q-P} \in \mathbb{F}$. $\square$

Definition: Lines L, M are said to be **perpendicular** (denoted $L \perp M$) if and only if $\mathrm{den}(L, M) = \text{-}1$.

Lemma 1.9. *Let $A \neq B$ be on L, $P \neq Q$ be on M, and $R \neq T$ be on N where L, M, N are lines.*

i) $L \perp M$ *iff* $\dfrac{P-Q}{A-B} \in \mathbb{I}$.

ii) $\mathbb{F} \perp L$ *iff* $L = \mathbb{I} + b$, $b \in \mathbb{E}$.

iii) *Assume* $M \perp N$. *Then* $L \parallel N$ *iff* $L \perp M$.

Proof: i) $L \perp M$ iff $\left(\frac{P-Q}{A-B}\right)\left(\frac{\overline{A}-\overline{B}}{\overline{P}-\overline{Q}}\right) = -1$ iff $\frac{P-Q}{A-B} = -\left(\frac{\overline{P}-\overline{Q}}{\overline{A}-\overline{B}}\right)$.

ii) If $L = \mathbb{I} + b$ and $t \in \mathbb{I}$, then $\frac{(t+b)-b}{1-0} = t \in \mathbb{I}$ and $\mathbb{F} \perp L$ by i). Conversely, $\mathbb{F} \perp L \implies \quad A - B = \frac{A-B}{1-0} \in \mathbb{I}$. Thus, $L = (A-B)\mathbb{F} + B = \mathbb{I} + B$.

iii) $M \perp N \implies \frac{R-T}{P-Q} \in \mathbb{I}$ by i). Thus,

$$L \perp M \iff \frac{P-Q}{A-B} \in \mathbb{I} \iff \frac{R-T}{A-B} = (\frac{R-T}{P-Q})(\frac{P-Q}{A-B}) \in \mathbb{F} \iff L \parallel N. \quad \square$$

Definition: Any line parallel to $\mathbb{I}$ will be called a **vertical line.**

By Lemma 1.9(ii,iii), we could equivalently define a vertical line to be any line perpendicular to $\mathbb{F}$.

Lemma 1.10.

i) *Given a line L and $p \in \mathbb{E}$, there is a unique line M with $p \in M$ and $L \parallel M$.*

ii) *Given a line L and $p \in \mathbb{E}$, there is a unique line M with $p \in M$ and $L \perp M$.*

Proof: WMA $L = \mathbb{F}$.

i) Now $L \parallel M$ iff $M = \mathbb{F} + b, b \in \mathbb{E}$. But $p \in M = \mathbb{F} + b \implies p = t + b$ for some $t \in \mathbb{F} \implies b = p - t \implies M = \mathbb{F} + (p - t) = \mathbb{F} + p$ since $t \in \mathbb{F}$.

ii) $M \perp \mathbb{F}$ iff $M = \mathbb{I}+b, b \in \mathbb{E}$. Now $p \in \mathbb{I}+b \implies p = t+b, t \in \mathbb{I} \implies b = p-t$, $t \in \mathbb{I} \implies M = \mathbb{I} + b = \mathbb{I} + (p - t) = \mathbb{I} + p$. □

Lemma 1.11. *Let $t \in L - \mathbb{F}$. The following are equivalent:*

i) *L is a vertical line.*

ii) *$\bar{t} \in L$.*

iii) *$L = \mathbb{I} + b, b \in \mathbb{F}$.*

Proof: We know L is vertical iff $L \perp \mathbb{F}$.

i) $\Leftrightarrow$ ii): Let M be the line passing through $t, \bar{t}$. Since $\bar{t} - t \in \mathbb{I}$, $M \perp \mathbb{F}$. By Lemma 1.10(ii), M is the unique line passing through t and perpendicular to $\mathbb{F}$. Thus, $L \perp \mathbb{F}$ iff $L = M$ iff $\bar{t} \in L$.

i) $\Leftrightarrow$ iii): Now iii) $\implies$ i) by Lemma 1.9(ii). If $L \perp \mathbb{F}$, then den(L,$\mathbb{F}$) $\neq 1$. Thus, $\exists\, t \in L \cap \mathbb{F} \neq \emptyset$. Since $\mathbb{I} + t$ is a line passing through t and perpendicular to $\mathbb{F}$ and L is the unique such line, we have $L = \mathbb{I} + t$. □

Note that $a \neq b \in \mathbb{E}^\times$ lie on the same vertical line iff $a + \bar{a} = b + \bar{b}$. ($\mathbb{I} + a = (\bar{a} - a)\mathbb{F} + a = (\bar{b} - b)\mathbb{F} + b = \mathbb{I} + b$ iff $a - b \in \mathbb{I}$.)

Define $\rho : \mathbb{E}^\times \to \mathbb{S}$ by $\rho(z) = z/\bar{z}$. Given $s \in \mathbb{S} - \{-1\}$,

$$\rho(1 + s) = \frac{1 + s}{1 + \bar{s}} = \frac{1 + s}{1 + \frac{1}{s}} = s.$$

Since $\rho(\mathbb{I} - \{0\}) = \{-1\}$, ρ is surjective. Also $\ker(\rho) = \mathbb{F}^\times$.

Note that den(L,M) $= \rho\left(\frac{P-Q}{A-B}\right)$ where $A \neq B \in L, P \neq Q \in M$.

Lemma 1.12. *Given a line L, $p \in L$ and $s \in \mathbb{S}$, there is a unique line M such that $p \in M$ and den(L,M) $= s$.*

Proof: WMA $L = \mathbb{F}$ and $p = -1$. If $s = -1$, then the result follows from Lemma 1.10(ii). Otherwise, let M be the line through p and s. Then den($\mathbb{F}$,M) $= \rho\left(\frac{s-(-1)}{1-0}\right) = s$. Suppose N is another line with $-1 \in N$ and den($\mathbb{F}$,N) $= s$. Let $-1 \neq t \in N$. Then

$$den(\mathbb{F}, M) = \frac{s+1}{\bar{s}+1} = \frac{t+1}{\bar{t}+1} = den(\mathbb{F}, N) \implies (s+1)(\overline{t+1}) = (\overline{s+1})(t+1)$$

Therefore, $M \parallel N$ which implies $M = N$ since $-1 \in M \cap N \neq \emptyset$. $\square$

Definition: C is said to be a **circle** in $\mathbb{E}$ iff it is the image of $\mathbb{S}$ under a Borel element. I.e., $C = a\mathbb{S} + b$ where $a \in \mathbb{E}^\times, b \in \mathbb{E}$.

Since B acts transitively on all circles in $\mathbb{E}$, there are

$$\frac{|B|}{|B_{\mathbb{S}}|} = \frac{(q^2-1)q^2}{q+1} = q^3 - q^2$$

distinct circles in $\mathbb{E}$ in the finite case. Moreover,

$$|a\mathbb{S} + b| = |\mathbb{S}| = \frac{|\mathbb{E}^\times|}{|\ker(\rho)|} = \frac{q^2-1}{q} = q+1$$

since ρ is surjective.

Definition: Let $x, y \in \mathbb{E}$. The **length** of x (or the **norm** of x) is denoted by $|x|^2$ and is defined by $|x|^2 = x\bar{x}$.

The **distance** between x and y is $|x-y|^2$.

Observe that if $x, y \in \mathbb{E}$ and $az + b \in B$, then

$$|(ax+b) - (ay+b)|^2 = |ax - ay|^2 = |a|^2|x-y|^2.$$

Thus, B preserves distances only up to a scalar multiple. Nevertheless, since all distances change by the same scalar, we may assume $P = 0, Q = 1$ (or $P = -1, Q = 1$, etc.) in proving statements about $|P - Q|^2$ with $P \neq Q$.

Lemma 1.13. $a\mathbb{S} + b = \{z \mid |z - b|^2 = |a|^2\}$.

Proof: Given $as + b$ with $s \in \mathbb{S}$, $|(as + b) - b|^2 = |as|^2 = |a|^2|s|^2 = |a|^2$ since $|s|^2 = 1$.

Conversely, assume $|z - b|^2 = |a|^2$. Let $w = \frac{z-b}{a}$. Then $z = aw + b$ and $|w|^2 = \frac{|z-b|^2}{|a|^2} = 1$. So $w \in \mathbb{S}$. $\square$

Definition: The circle $C = a\mathbb{S} + b$ has **center** b and **sqradius** (denoted $\mathrm{sqr}(C)$) $a\bar{a}$.

In particular, $\mathbb{S}$ and $\mathbb{T}$ are the circles centered at 0 with sqradii 1,-1 respectively.

Lemma 1.14.

i) *Any three distinct noncollinear points lie on a unique circle.*

ii) *A line and a circle can intersect at at most two points.*

iii) *Any two distinct circles intersect at at most two points.*

Proof: i) Any circle C is completely determined by its center W and one point A on the circle ($\implies$ $\mathrm{sqr}(C) = |W - A|^2$). It thus suffices to show that there is exactly one point W equidistant from P, Q and R. Now W must satisfy

$$|W - P|^2 = |W - Q|^2 = |W - R|^2.$$

By the observation above, WMA $P = 0, Q = 1$. Thus,

$$W\overline{W} = W\overline{W} - \overline{W} - W + 1 = W\overline{W} - R\overline{W} - \overline{R}W + R\overline{R}$$

which implies $\overline{W} + W - 1 = 0 = R\overline{W} + \overline{R}W - R\overline{R}$. The unique solution to these equations is $W = \frac{R\overline{R}-R}{\overline{R}-R}$. ($W$ exists since $R \notin \mathbb{F}$.)

ii) Let $L = a\mathbb{F} + b$. Since

$$L \cap \mathbb{S} = \{at + b \mid a\overline{a}t^2 + (\overline{a}b + a\overline{b})t + (b\overline{b} - 1) = 0, t \in \mathbb{F}\},$$

$|L \cap \mathbb{S}| \leq 2$. Consequently, $|L \cap C| \leq 2$ for any circle C.

iii) By part i), two distinct circles can't intersect at three distinct points unless the three points are collinear. But three collinear intersection points would give a contradiction to part ii). $\square$

Remarks: i) If $P \in C$, a circle centered at R, then $(PR) \cap C = \{P, 2R - P\}$. I.e., a line passing through the center of a circle cannot intersect the circle in only one point.

ii)It is possible for a line to pass through the center of a circle without intersecting the circle. For instance, $\mathbb{F}$ passes through the center 0 of $\mathbb{T}$ but $\mathbb{F} \cap \mathbb{T} = \emptyset$ when $-1 \notin \mathbb{E}_+$. In fact, exactly half the lines through the center of a circle intersect the circle in the finite case. (WMA the circle is $\mathbb{S}$. There are exactly $q+1$ lines through 0. Any line passing through 0 and intersecting $\mathbb{S}$ must intersect it at two points by Remark i). Thus, there are $\frac{q+1}{2}$ lines passing through 0 and intersecting $\mathbb{S}$.)

Definition: A line L is said to be **tangent** to a circle C if L intersects C at exactly one point.

Lemma 1.15.

i) *Given $P \neq Q$, there is a unique circle with center P passing through Q.*

ii) *Given $P \notin L$, there is a unique circle C with center P and L tangent to C.*

iii) *Given a circle C and $P \in C$, there is a unique line through P and tangent to C.*

Proof: i) WMA $P = 0, Q = 1$. Now any circle centered at 0 is of the form

$$a\mathbb{S} = \{z \mid |z|^2 = |a|^2\}.$$

Thus, $1 \in a\mathbb{S}$ iff $|a|^2 = 1$ iff $a \in \mathbb{S}$ iff $a\mathbb{S} = \mathbb{S}$.

ii) WMA $L = \mathbb{F}$. Any circle centered at P is of the form $a\mathbb{S} + P = \{z \mid |z - P|^2 = a\overline{a}\}$. Now

$$\mathbb{F} \cap (a\mathbb{S} + P) = \{ax + p \mid x \in \mathbb{S}, ax^2 + (P - \overline{P})x - \overline{a} = 0\}.$$

The quadratic equation $ax^2 + (P - \overline{P})x - \overline{a} = 0$ has a unique solution iff the discriminant

$$\Delta = (P - \overline{P})^2 + 4a\overline{a} = 0 \iff a\overline{a} = \frac{(P - \overline{P})^2}{-4}.$$

Thus, $C = \{z \mid |z - P|^2 = \frac{(P-\overline{P})^2}{-4}\}$ is the unique circle centered at P which is tangent to $\mathbb{F}$ (at $\frac{P+\overline{P}}{2}$).

iii) WMA $P = 0$. Then $C = b\mathbb{S} + b = \{z \mid |z - b|^2 = |b|^2\}$. Any line through 0 must be of the form $a\mathbb{F}$. Let $\lambda = \frac{\bar{a}b}{a\bar{b}}$. Then

$$(a\mathbb{F}) \cap (b\mathbb{S} + b) = \{b(s+1) \mid s \in \mathbb{S}, \lambda s^2 + (\lambda - 1)s - 1 = 0\}.$$

The quadratic equation has a unique solution iff $\Delta = (\lambda-1)^2 + 4\lambda = (\lambda+1)^2 = 0$ iff $\lambda = -1$ iff $a\bar{b} \in \mathbb{I} - \{0\}$. Now $a\bar{b}, c\bar{b} \in \mathbb{I} - \{0\} \implies ac^{-1} = \frac{a\bar{b}}{c\bar{b}} \in \mathbb{F} \implies a\mathbb{F} = c\mathbb{F}$. Thus, $\left(\frac{b-\bar{b}}{\bar{b}}\right)\mathbb{F}$ is the unique line through 0 and tangent to C if $b \notin \mathbb{F}$. If $b \in \mathbb{F}$, then $\mathbb{I}$ is the unique such line. $\square$

We will denote the unique tangent line to C at p by $T_p(C)$.

We now show that every element of $\mathbb{E}^\times - \mathbb{I}$ has a "polar coordinate representation". That is, every element of $\mathbb{E}^\times - \mathbb{I}$ can be written uniquely in the form tx where $t \in \mathbb{F}^\times$ and $x \in (\mathbb{S}+1) - \{0\}$.

Proposition 1.16. $\mathbb{E}^\times - \mathbb{I} = \mathbb{F}^\times((\mathbb{S}+1) - \{0\})$.

Proof: Let $z \in \mathbb{E}^\times - \mathbb{I}$. Let L be the line passing through $0, z$. Since $0 \in L \cap (\mathbb{S}+1)$ and $\mathbb{I}$ is the unique such line through 0 and tangent to $\mathbb{S}+1$ (by Lemma 1.15(iii)), there's another point $x \in L \cap (\mathbb{S}+1)$. Since $0, x \in L$, $L = x\mathbb{F}$. Thus, $z = xt$ for some $t \in \mathbb{F}^\times$. If $z = \lambda w$ where $\lambda \in \mathbb{F}^\times$ and $w \in ((\mathbb{S}+1) - \{0\})$, then $w = x\left(\frac{t}{\lambda}\right) \in L$. Since $\{0, x\} = L \cap (\mathbb{S}+1)$, $w = x$ and $\lambda = t$. $\square$

Remark: Analogously, $\mathbb{E} - \mathbb{F} = \mathbb{F}^\times((a\mathbb{S} + a) - \{0\})$ where $a \in \mathbb{I} - \{0\}$. Thus, elements of $\mathbb{E} - \mathbb{F}$ can also be represented by polar coordinates.

Lemma 1.17.

i) *Let $C = a\mathbb{S} + b, p \in C - \mathbb{F}$. Then $b \in \mathbb{F}$ iff $\bar{p} \in C$.*

ii) *Let* $C = a\mathbb{S} + b, b \neq 0$. *If* $x \neq y \in (b\mathbb{F}^\times) \cap C$, *then* $|x|^2 \neq |y|^2$.

Proof: i) If $b \in \mathbb{F}$, then WMA $b = 0$. So $C = a\mathbb{S}$ and $p = as$ for some $s \in \mathbb{S}$. Then $\overline{p} = \overline{as} = a\left[s\left(\frac{\overline{as}}{as}\right)\right] \in a\mathbb{S}$ since $s, \frac{\overline{as}}{as} \in \mathbb{S}$.

Conversely, $\overline{p} \in C \implies |p - b|^2 = |\overline{p} - b|^2 \implies$

$$p\overline{p} - b\overline{p} - p\overline{b} + b\overline{b} = (p - b)(\overline{p - b}) = (\overline{p} - b)(\overline{\overline{p} - b}) = p\overline{p} - bp - \overline{bp} + b\overline{b}.$$

Thus, $(p - \overline{p})(b - \overline{b}) = 0$ and $b \in \mathbb{F}$ since $p \notin \mathbb{F}$.

ii) Now $x = br, y = at$ where $r, t \in \mathbb{F}^\times$. Thus, $|x|^2 = b\overline{b}r^2 = b\overline{b}t^2 = |y|^2$ iff $r = \pm t$ iff $y = \pm x$. The equation $|b - br|^2 = |b + br|^2 \implies (1 - r)^2 = (1 + r)^2 \implies r = 0$, a contradiction. Thus, $|x|^2 = |y|^2$ since $-x \notin C$. $\square$

Remark: In the finite case, $|C| = q + 1$ and $|\mathbb{F}| = q$. Thus, $C - \mathbb{F}$ is always nonempty in Lemma 1.17(i).

We now prove the analogs of some classical geometry theorems.

Proposition 1.18. *Let* L, M, N *be lines with* $L \cap N = \{A\}$ *and* $M \cap N = \{B\}$. *Then* $L \parallel M$ *iff den(L,N) = den(M,N).*

Proof: If $A = B$, then $L \parallel M$ iff $L = N$ iff den(L,N) = den(M,N) (by Lemma 1.12). Thus, WMA $A \neq B$. Let $P \neq A \in L, Q \neq B \in M$. Then

$$den(L, N) = \left(\frac{A - B}{A - P}\right)\left(\frac{\overline{A} - \overline{P}}{\overline{A} - \overline{B}}\right) = \left(\frac{A - B}{Q - B}\right)\left(\frac{\overline{Q} - \overline{B}}{\overline{A} - \overline{B}}\right) = den(M, N)$$

iff $(A - B)(\overline{Q - B}) = (\overline{A - P})(Q - B)$ iff $L \parallel M$. $\square$

Proposition 1.19.

Assume $L \cap M = \{p\}$, $L \cap \widetilde{L} = \{Q\}$, *and* $M \cap \widetilde{M} = \{R\}$ *where* $L \perp \widetilde{L}$, $M \perp \widetilde{M}$. *Then den(L,M) = den(*$\widetilde{L}$*,* $\widetilde{M}$*).*

Proof: WMA $P = 0$ and $L = \mathbb{F}$. Let $R \neq U \in M, Q \neq V \in \widetilde{L}, R \neq W \in \widetilde{M}$. Now

$$L \perp \widetilde{L} \implies \frac{Q-V}{\overline{Q}-\overline{V}} = -1 \text{ and } M \perp \widetilde{M} \implies \left(\frac{R-W}{R-U}\right)\left(\frac{\overline{R}-\overline{U}}{\overline{R}-\overline{W}}\right) = -1.$$

Therefore, $\text{den}(\widetilde{L}, \widetilde{M}) = \left(\frac{R-W}{Q-V}\right)\left(\frac{\overline{Q}-\overline{V}}{\overline{R}-\overline{W}}\right) = \frac{R-U}{\overline{R}-\overline{U}} = \text{den}(L,M)$. $\square$

Proposition 1.20. *If* P, Q, R *are distinct on a circle* C *with center* W, *then* $den(WP, WQ) = [den(RP, RQ)]^2$.

Proof: WMA $C = \mathbb{S}$. Then $W = 0$. Since $P, Q, R \in \mathbb{S}$,

$$den(RP, RQ) = \left(\frac{R-Q}{R-P}\right)\left(\frac{\overline{R-P}}{\overline{R-Q}}\right) = \left(\frac{R-Q}{R-P}\right)\left(\frac{P-R}{PR}\right)\left(\frac{QR}{Q-R}\right) = \frac{Q}{P}$$

and $\text{den}(0P, 0Q) = \frac{Q\overline{P}}{P\overline{Q}} = \frac{Q^2}{P^2}$. $\square$

Observe that if L, M, N are lines then

$$den(L, N) = den(L, M)den(M, N).$$

(Let $P \neq Q \in L, R \neq S \in M, T \neq W \in N$. Then

$$\left(\frac{T-W}{P-Q}\right)\left(\frac{\overline{P}-\overline{Q}}{\overline{T}-\overline{W}}\right) = \left(\frac{R-S}{P-Q}\right)\left(\frac{\overline{P}-\overline{Q}}{\overline{R}-\overline{S}}\right)\left(\frac{T-W}{R-S}\right)\left(\frac{\overline{R}-\overline{S}}{\overline{T}-\overline{W}}\right).)$$

Definition: Let L, M be lines with $L \cap M = \{p\}$. A line N is said to **bisect** den(L,M) at p if $p \in N$ and den(L,N) = den(N,M).

If N exists, it is unique.

Proposition 1.21. *Let L, M be lines with $L \cap M = \{p\}$. Let $\beta = den(L,M)$. Then β can be bisected at p iff $\beta \in \mathbb{S}_+$.*

Proof: If $\exists$ N s.t. $den(L,N) = den(N,M)$, then

$$\beta = den(L,N)den(N,M) = [den(L,N)]^2 \in \mathbb{S}_+.$$

Conversely, assume $\beta = \gamma^2 \in \mathbb{S}_+$. By Lemma 1.12, there is a unique line N with $p \in N$ and $den(L,N) = \gamma$. Then $den(N,M) = \frac{den(L,M)}{den(L,N)} = \gamma$ also and N bisects β at p. $\square$

The set of points in $\mathbb{E}$ fixed pointwise by the maps $z \mapsto \overline{z}, z \mapsto 1/\overline{z}$ are $\mathbb{F}, \mathbb{S}$ respectively.

Definition: The **reflection** about a line L (denoted r_L) is $g\overline{z}g^{-1}$ where $g \in B$ sends $\mathbb{F}$ to L. Similarly, the **inversion** about a circle C (denoted r_C) is $h(1/\overline{z})h^{-1}$ where $h \in B$ sends $\mathbb{S}$ to C.

Remarks: i) Note that $B_{\mathbb{F}}$ commutes with $z \mapsto \overline{z}$ and $B_{\mathbb{S}}$ commutes with $z \mapsto 1/\overline{z}$.

Thus, reflections (resp. inversions) are well-defined since $g\mathbb{F} = L = h\mathbb{F}$ (respectively $g\mathbb{S} = C = h\mathbb{S}$) $\implies h = gf$ with $f \in B_{\mathbb{F}}$ (resp. $f \in B_{\mathbb{S}}$).

ii) The set of points in $\mathbb{E}$ fixed pointwise by r_L, r_C is L, C respectively. We call this fixed point set the **mirror** of the reflection/inversion.

iii) Reflections and inversions have order two.

Any reflection is of the form

$$(az+b)\circ\overline{z}\circ(az+b)^{-1} = (az+b)\circ\overline{z}\circ\left(\frac{z-b}{a}\right) = (az+b)\circ\left(\frac{\overline{z}-\overline{b}}{\overline{a}}\right) = \frac{a}{\overline{a}}\overline{z}+(b-\frac{a\overline{b}}{\overline{a}}).$$

The mirror of this reflection is $a\mathbb{F}+b$.

Any inversion is of the form

$$(az+b)\circ(1/\overline{z})\circ(az+b)^{-1} = (az+b)\circ(1/\overline{z})\circ\left(\frac{z-b}{a}\right) = (az+b)\circ\frac{\overline{a}}{\overline{z}-\overline{b}} = \frac{a\overline{a}}{\overline{z}-\overline{b}}+b.$$

The mirror of this inversion is $a\mathbb{S}+b$.

We have thus shown the following.

Lemma 1.22. *If $L = a\mathbb{F}+b$ and $C = a\mathbb{S}+b$, then*

$$r_L(z) = \frac{a}{\overline{a}}\overline{z} + (b - \frac{a\overline{b}}{\overline{a}}) \text{ and } r_C(z) = \frac{a\overline{a}}{\overline{z}-\overline{b}} + b.$$

Notice that r_C interchanges the center b of C and ∞.

Lemma 1.23.

i) *Reflections (inversions) preserve lines (circles).*

ii) *Reflections conjugate dengles. I.e., if L, M, N are lines with $M \cap N \neq \emptyset$, then den($r_L(M)$,$r_L(N)$) = 1/den(L,M).*

Proof: Now $r_L = g \circ \overline{z} \circ g^{-1}$ and $r_C = h \circ (1/\overline{z}) \circ h^{-1}$.

i) Since we already know Borel elements take lines to lines and circles to circles, it suffices to show the statement for $r_L(z) = \overline{z}, r_C(z) = 1/\overline{z}$. Let $L = a\mathbb{F}+b, C = a\mathbb{S}+b$. Then $r_L(a\mathbb{F}+b) = (\overline{a})\mathbb{F}+\overline{b}$ and

$$r_C(a\mathbb{S}+b) = (\frac{1}{\overline{a}})\mathbb{S} + \frac{1}{\overline{b}} \text{ if } b \neq 0 \text{ and } (\frac{1}{\overline{a}})\mathbb{S} \text{ if } b = 0.$$

ii) Since elements of B preserve the dengle, it suffices to show that $r_L(z) = \overline{z}$ inverts dengles. Let $A \neq B \in M, P \neq Q \in N$. Then

$$den(r_L(M), r_L(N)) = \left(\frac{\overline{P} - \overline{Q}}{\overline{A} - \overline{B}}\right)\left(\frac{A - B}{P - Q}\right) = \frac{1}{den(M, N)}. \quad \square$$

Lemma 1.24. *If L, M are two lines with $L \cap M = \{0\}$, then $r_M \circ r_L(z) =$ [den(L,M)]z.*

Proof: Since $0 \in L \cap M, L = a\mathbb{F}, M = t\mathbb{F}$. Thus, $r_L(z) = (\frac{a}{\overline{a}})\overline{z}$ and $r_M(z) = (\frac{t}{\overline{t}})\overline{z}$. Thus, $r_M \circ r_L(z) = (\frac{t}{\overline{t}})(\frac{\overline{a}}{a})z = [\text{den}(L,M)]z$. $\square$

Lemma 1.25. *Let L, M be distinct lines, C a circle.*

i) *$r_L(M) = M$ iff $L \perp M$.*

ii) *$r_L(C) = C$ iff the center of C lies on L.*

Proof: i) WMA $L = \mathbb{F}$. Then $r_L(z) = \overline{z}$. Note that both conditions of the statement imply that $\mathbb{F} \cap M \neq \emptyset$. (If $L \parallel M$, then $M = \mathbb{F} + b$ where $b \in \mathbb{E} - \mathbb{F}$. If $\overline{b} \in M$, then $\overline{b} = a + b$ for some $a \in \mathbb{F}$ and $a = \overline{b} - b \in (\mathbb{I} - \{0\}) \cap \mathbb{F} = \emptyset$.) Let $p \in \mathbb{F} \cap M$. Let $Q \in M - \mathbb{F}$. Then $r_L(M) = M$ iff $\overline{z}(PQ) = P\overline{z}(Q) = PQ$ iff $\overline{z}(Q) \in M$ iff $M \perp \mathbb{F}$ by Lemma 1.11.

ii) Now $g(C) = \mathbb{S}$ for some $g \in B$. Since $r_{g(L)} = g \circ r_L \circ g^{-1}$ and g takes the center of C to the center of $\mathbb{S}$, WMA $C = \mathbb{S}$. Let $L = a\mathbb{S} + b$. Then $r_L(z) = a\left(\frac{\overline{z} - \overline{b}}{\overline{a}}\right) + b$. If $0 \in L$, then $b = 0$ and $r_L(z) = (\frac{a}{\overline{a}})\overline{z}$. Given $x \in \mathbb{S}, r_L(z)\overline{r_L(z)} = \left(\frac{a}{\overline{a}}\overline{x}\right)\left(\frac{\overline{a}}{a}x\right) = x\overline{x} = 1$. Therefore, $r_L(x) \in \mathbb{S}$ and $r_L(\mathbb{S}) \subseteq \mathbb{S}$. Since r_L has order two, $r_L(\mathbb{S}) = \mathbb{S}$.

Conversely, if $r_L(\mathbb{S}) = \mathbb{S}$, then $r_L(1) = \frac{a-a\overline{b}+\overline{a}b}{\overline{a}}, r_L(-1) = \frac{-a-a\overline{b}+\overline{a}b}{\overline{a}} \in \mathbb{S}$. Now $r_L(1)\overline{r_L(1)} = 1 = r_L(-1)\overline{r_L(-1)}$

$$\Longrightarrow \frac{(a - a\overline{b} + \overline{a}b)(\overline{a} - \overline{a}b + a\overline{b})}{a\overline{a}} = \frac{(-a - \overline{a}b + a\overline{b})(-a - a\overline{b} + \overline{a}b)}{a\overline{a}}$$

$$\Longrightarrow -2a\overline{a}b + 2aa\overline{b} - 2a\overline{a\overline{b}} + 2\overline{a}\overline{a}b = 0$$

$$\Longrightarrow -\overline{a}b(a - \overline{a}) + a\overline{b}(a - \overline{a}) = 0$$

$$\Longrightarrow (a\overline{b} - \overline{a}b)(a - \overline{a}) = 0 \Longrightarrow a\overline{b} = \overline{a}b \text{ or } a = \overline{a}.$$

If $a\overline{b} = \overline{a}b$, then $r_L(0) = \frac{b\overline{a}-a\overline{b}}{\overline{a}} = 0 \Longrightarrow 0 \in L$. If $a = \overline{a}$, then $L = a\mathbb{F} + b = \mathbb{F} + b$. Since $r_L(1) = 1 - \overline{b} + b \in \mathbb{S}$, we have $b(\overline{b} - b) = 0$. Thus, either $b = 0$ or $b \in \mathbb{F}$. In either case, $L = \mathbb{F}$ and $0 \in L$. $\square$

Lemma 1.26. *(Essential Uniqueness of Distances) Assume C is a circle centered at R and $p \notin C, p \neq R$. If $Q \neq T \in C$ with $|P - Q|^2 = |P - T|^2$, then $T = r_L(Q)$ where L is the line through R and P.*

Proof: WMA $P = 0$. Since $|Q - 0|^2 = |T - 0|^2$, Q and T both lie on the circle G centered at 0 of sqradius $Q\overline{Q}$. Since $Q \neq T, C \cap G = \{Q, T\}$. But since L passes through the center of both C and G, $r_L(C) = C$ and $r_L(G) = G$ (by Lemma 1.25). So $r_L(Q), r_L(T) \in C \cap G$. If $r_L(Q) = Q$ and $r_L(T) = T$, then $Q, T \in L$. This is a contradiction to Lemma 1.17(ii) since $|Q - 0|^2 = |T - 0|^2$. Thus, $r_L(Q) = T$. $\square$

Thus, each distance $|P - Q|^2, Q \in C$ occurs exactly twice except for the distances $|P - X|^2, |P - Y|^2$ where $X, Y \in L \cap C$ (which occur exactly once).

Definition: Let $C = a\mathbb{S} + b$. An element $r \in B$ such that $r(b) = b$ and $r(C) = C$ is said to be a **rotation** with respect to C.

Lemma 1.27. *Given $x, y \in C = a\mathbb{S}+b$, there is a unique rotation r with respect to C with $r(x) = y$.*

Proof: WMA $C = \mathbb{S}$. Consider $r(z) = \left(\frac{y}{x}\right) z$. Then $r(0) = 0, r(x) = \left(\frac{y}{x}\right) x = y$ and $r \in B_{\mathbb{S}}$ (since $\frac{y}{x} \in \mathbb{S}$). If $t(z) = qz \in B_{\mathbb{S}}$ and $t(x) = y$, then $q = \frac{y}{x}$ so $t = r$ and r is unique. $\square$

We have seen that the Borel group preserves dengles and ratios of lengths, but preserves distances only up to a scalar multiple. We will now determine what type of elements preserve $|\ \ |^2$.

Definition: An element $g : \mathbb{E} \to \mathbb{E}$ such that $|g(x) - g(y)|^2 = |x - y|^2$ is said to be an **isometry** of $\mathbb{E}$.

The isometries of $\mathbb{E}$ form a group under composition, denoted $\mathrm{Isom}(\mathbb{E})$.

Lemma 1.28. *If $g : \mathbb{E} \to \mathbb{E}$ with $g(0) = 0$, $g(1) = 1$ and $|g(x)-g(y)|^2 = |x-y|^2$, then $g = 1$ or $g(z) = \overline{z}$ for all $z \in \mathbb{E}$.*

Proof: Let $P \in \mathbb{E} - \{0, 1\}$. Let

$$R = \{z \mid |z|^2 = |P|^2\}, \quad T = \{z \mid |z - 1|^2 = |P - 1|^2\}.$$

Since $R \neq T$ (the centers are distinct) and $P \in R \cap T$, we know $|R \cap T| = 1$ or $|R \cap T| = 2$.

We also note that $g(P) \in R \cap T$ since g fixes 0 and 1:

$$|g(P)|^2 = |g(P)-g(0)|^2 = |P-0|^2 = |P|^2 \text{ and } |g(P)-1|^2 = |g(P)-g(1)|^2 = |P-1|^2.$$

Case 1. $P = \overline{P}$

Suppose there exists $P \neq Q \in R \cap T$. Now Q must satisfy $Q\overline{Q} = P\overline{P} = P^2$ and $Q\overline{Q} - Q - \overline{Q} + 1 = P^2 - 2P + 1$. Thus, $Q + \overline{Q} = 2P$. But $\overline{Q} = Q$ since $\overline{Q} \in R \cap T$ (by Lemma 1.17(i)). Thus, $Q = P$ and $R \cap T = \{P\}$. In particular, $g(P) = P$.

Case 2. $P \neq \overline{P}$

Then $R \cap T = \{P, \overline{P}\}$ so that $g(P) = P$ or $g(P) = \overline{P}$.

The above shows that $g(z) = z \; \forall \; z \in \mathbb{F}$. If $g(z) = z \; \forall \; z \in \mathbb{E}$, then $g = 1$. Otherwise, $\exists \; P \in \mathbb{E} - \mathbb{F}$ with $g(P) = \overline{P}$. We'll show that $g(z) = \overline{z} \; \forall \; P \neq z \in \mathbb{E} - \mathbb{F}$.

Note that $x \mapsto \overline{x}$ is in Isom($\mathbb{E}$). Thus,

$$|z - P|^2 = |g(z) - g(P)|^2 = |\overline{g(z)} - \overline{g(P)}|^2 = |\overline{g(z)} - P|^2.$$

If $g(z) = z$, then we have $|z - P|^2 = |\overline{z} - P|^2$. This is impossible since $z, P \in \mathbb{E} - \mathbb{F}$ (because $|z - P|^2 = |\overline{z} - P|^2$ iff $(\overline{z} - z)(P - \overline{P}) = 0$). Thus, $g(z) = \overline{z}$. $\square$

Theorem 1.29. *Isom(* $\mathbb{E}$ *)* $= \langle \mathbb{S}z + \mathbb{E}, \overline{z} \rangle$.

Proof: Now $|(ax + b) - (ay + b)|^2 = |a|^2 |x - y|^2 = |x - y|^2$ when $a \in \mathbb{S}$. Thus, $\langle \mathbb{S}z + \mathbb{E}, \overline{z} \rangle \subseteq$ Isom($\mathbb{E}$) since $\mathbb{S}z + \mathbb{E}$ and $z \mapsto \overline{z}$ are isometries and Isom($\mathbb{E}$) is closed under composition.

Let $g \in$ Isom($\mathbb{E}$). Let

$$h(z) = \frac{g(z) - g(0)}{g(1) - g(0)} = \frac{z}{g(1) - g(0)} \circ (z - g(0)) \circ g(z).$$

Then $h(z) \in \mathrm{Isom}(\mathbb{E})$ since it is a composition of $g(z)$ and two elements of $\mathbb{S}z+\mathbb{E}$. Also $h(0) = 0, h(1) = 1$. By Lemma 1.28, $h = 1$ or $h(z) = \overline{z}$. Thus,

$$g(z) = (z - g(0))^{-1} \circ \left(\frac{z}{g(1) - g(0)}\right)^{-1} \circ h(z) \in \langle \mathbb{S}z + \mathbb{E}, \overline{z} \rangle . \quad \square$$

Corollary 1.30. *The isometries of* $\mathbb{E}$ *are bijections.*

Remark: Note that B normalizes $\mathrm{Isom}(\mathbb{E})$: Given $g \in \mathrm{Isom}(\mathbb{E})$ and $h(z) = az + b$,

$$\begin{aligned} |hgh^{-1}(w) - hgh^{-1}(z)|^2 &= |a|^2 |gh^{-1}(w) - gh^{-1}(z)|^2 \\ &= |a|^2 |h^{-1}(w) - h^{-1}(z)|^2 = |a|^2 \left(\frac{1}{|a|^2}\right) |w - z|^2 = |w - z|^2. \end{aligned}$$

In particular, every reflection and rotation is an isometry since it can be written in the form $g\overline{z}g^{-1}$, $g(kz)g^{-1}$ respectively where $g \in B$, $k \in \mathbb{S}$.

Lemma 1.31. *Let* $g \in$ *Isom(*$\mathbb{E}$*).*

i) *If* g *fixes* $P \neq Q$ *and* $g \neq 1$, *then* g *is the reflection with mirror* PQ.

ii) *If* g *fixes three non-collinear points, then* $g = 1$.

Proof: WMA $P = 0, Q = 1$. (The element $h^{-1}gh \in \mathrm{Isom}(\mathbb{E})$ fixes 0,1 where $h \in B$ with $h(0) = P$ and $h(1) = Q$.) Then $PQ = \mathbb{F}$. By Lemma 1.28, $g = 1$ or $g(z) = \overline{z}$.

i) Since $g \neq 1, g(z) = \overline{z}$ and is thus the reflection with mirror $\mathbb{F}$.

ii) Let β be the third fixed point. Since $\beta \in \mathbb{F}, \overline{\beta} \neq \beta$. Thus, $g(\beta) = \beta \neq \overline{\beta}$ and $g(z) \neq \overline{z}$. Hence, $g = 1$. $\square$

Definition: Assume $P \neq Q \in \mathbb{E}$. The unique line passing through $\dfrac{P+Q}{2}$ (the **midpoint** of P and Q) and perpendicular to PQ is the **perpendicular bisector** of PQ.

Lemma 1.32.

i) *Assume $P \neq Q$, $A \neq B$ with $|A-P|^2 = |B-P|^2$ and $|A-Q|^2 = |B-Q|^2$. Then PQ is the perpendicular bisector of AB and $r_{PQ}(A) = B$.*

ii) *Let $A \neq B \in \{z \mid |z-P|^2 = |r|^2\} \cap \{z \mid |z-Q|^2 = |s|^2\}$ where $P \neq Q$. Then PQ is the perpendicular bisector of AB and $r_{PQ}(A) = B$.*

iii) *If $B \neq C \in \mathbb{E}$, let L be the perpendicular bisector of the line through B and C. Then $r_L(a\mathbb{S}+B) = a\mathbb{S}+C$.*

Proof: WMA $A = -1$, $B = 1$. Then $|-1-Q|^2 = |1-Q|^2 \implies Q + \overline{Q} = 0 \implies Q \in \mathbb{I}$. Similarly, $P \in \mathbb{I}$. Thus, $PQ = \mathbb{I}$ and is therefore the perpendicular bisector of AB. We have $r_{PQ}(z) = -\overline{z}$ so that $r_{PQ}(-1) = 1$.

ii) Now $|A-P|^2 = |B-P|^2$ and $|A-Q|^2 = |B-Q|^2$. The result thus follows from i).

iii) Given $x \in a\mathbb{S}+B$, $|r_L(x) - C|^2 = |r_L(x) - r_L(B)|^2 = |x-B|^2 = a\overline{a}$. $\square$

Theorem 1.33. *Every isometry of $\mathbb{E}$ is a product of at most three reflections.*

Proof: Let $\phi \in \mathrm{Isom}(\mathbb{E})$. If $\phi(0) = 0$, let $\rho := 1$. Otherwise, let $\rho := r_L$ where L is the perpendicular bisector of $\phi(0)$ and 0. Then $\rho(0) = \phi(0)$ by Lemma 1.32. Note that $s := \rho \circ \phi(1) \in \mathbb{S}$ since $\rho \circ \phi$ is an isometry fixing 0, the center of $\mathbb{S}$.

Let $\tau := 1$ if $s = 1$, $\tau := -\overline{z}$ if $s = -1$ and $\tau := r_{0(s+1)}$ otherwise. In the latter case, $0(s+1)$ is the perpendicular bisector of the line $1s$ (by Lemma 1.32) and thus $r_{0(s+1)}(s) = 1$. Thus, in all cases $\tau \circ \rho \circ \phi$ fixes 0 and 1. Then $\tau \circ \rho \circ \phi = 1$ or $\tau \circ \rho \circ \phi = \bar{z}$ by Lemma 1.28. Hence, $\phi = \rho \circ \tau$ or $\phi = \rho \circ \tau \circ \bar{z}$. $\square$

The above proof shows that any isometry of $\mathbb{E}$ fixing 0 is a product of two reflections.

Corollary 1.34. *Every rotation is a product of two reflections.*

Proof: Let g be a rotation. Then $g = h(kz)h^{-1}$ for $h \in B, k \in \mathbb{S}$. Since $kz = r_1 \circ r_2$ for reflections r_1 and r_2, $g = (hr_1h^{-1}) \circ (hr_2h^{-1})$. $\square$

Definition: Let P, Q, R be distinct noncollinear points of $\mathbb{E}$. The union of the three lines PQ, QR, RP (denoted $\triangle PQR$) is called a **triangle** in $\mathbb{E}$. P, Q, R are the **vertices** and the lines PQ, QR, RP are the **sides** of the triangle. The vertex P is said to be **opposite** the side QR and $\dfrac{Q+R}{2}$ is the **midpoint** of side QR.

We will use the notation $\triangle(P, Q, R)$ to denote the **oriented** triangle with vertices P, Q, R and dengles den(PQ,QR), den(QR,RP), den(RP,PQ).

A dengle equal to -1 is called a **right dengle**. A triangle with at least one right dengle is a **right triangle**.

Notice that the product of the dengles of any oriented triangle is one.

Theorem 1.35. *(Thales) If P, Q, R are distinct points, then den(PQ,QR) = -1 if and only if Q is on the circle C with center $\dfrac{P+R}{2}$ and passing through P and R.*

Proof: WMA $P = 1, R = -1$. Then $\dfrac{P+R}{2} = 0$ and $C = \mathbb{S}$. Thus,

$$den(PQ, QR) = -1 \iff \frac{Q+1}{Q-1} \in \mathbb{I} - \{0\} \iff Q\overline{Q} = 1 \iff Q \in \mathbb{S}. \quad \square$$

Theorem 1.36. *(Pythagorean Theorem) If P, Q, and R are distinct points, then den(PQ,QR) = -1 if and only if $|P-Q|^2 + |Q-R|^2 = |P-R|^2$.*

Proof: WMA $Q = 0$. Then

$$\begin{aligned}
|P-Q|^2 + |Q-R|^2 &= |P-R|^2 \\
&\iff P\overline{P} + R\overline{R} = P\overline{P} - P\overline{R} - \overline{P}R + R\overline{R} \\
&\iff PR = -\overline{P}R \iff \frac{R\overline{P}}{\overline{P}\overline{R}} = -1 \\
&\iff den(PQ, QR) = -1. \qquad \square
\end{aligned}$$

Proposition 1.37. *Let D, E be the midpoints of the sides AB, AC of $\triangle ABC$. Then $DE \parallel BC$ and $|D-E|^2 = \dfrac{|B-C|^2}{4}$.*

Proof: Since $D = \dfrac{A+B}{2}$ and $E = \dfrac{A+C}{2}$, $D - E = \dfrac{B-C}{2}$. The proof is therefore immediate since

$$den(BC, DE) = \left(\frac{D-E}{B-C}\right)\left(\frac{\overline{B}-\overline{C}}{\overline{D}-\overline{E}}\right). \quad \square$$

Definition: A line through a vertex of a triangle and the midpoint of the opposite side is a **median**.

Lemma 1.38. *In $\triangle(A, B, C)$, den(BC,AC) = den(AC,AB) if and only if the median through B is the perpendicular bisector of AC.*

Proof: Let M be the median through B. WMA $A = -1$ and $C = 1$. Then $0 \in M$. Now

$$
\begin{aligned}
den(BC, AC) = den(AC, AB) &\iff \left(\frac{2}{B-1}\right)\left(\frac{\overline{B}-1}{2}\right) = \left(\frac{B+1}{2}\right)\left(\frac{2}{\overline{B}+1}\right) \\
&\iff \overline{B}^2 - 1 = B^2 - 1 \iff \left(\frac{\overline{B}}{B}\right)^2 = 1 \\
&\iff \frac{\overline{B}}{B} = \pm 1 \iff B \in \mathbb{I} \cup \{0\} \ \ (\text{ since } B \notin \mathbb{F}\text{ }).
\end{aligned}
$$

Since $0 \in M$ and $AC = \mathbb{F}$, M is the perpendicular bisector of AC iff $M \perp \mathbb{F}$ iff $M = \mathbb{I}$ iff $B \in \mathbb{I} - \{0\}$. $\square$

Definition: We say that $\triangle ABC$ is **isosceles** if $|A - B|^2 = |B - C|^2$ and **equilateral** if $|A - B|^2 = |B - C|^2 = |A - C|^2$.

Theorem 1.39. *The $\triangle ABC$ is isosceles ($|A - B|^2 = |B - C|^2$) if and only if den(BC,AC) = den(AC,AB).*

Proof: Let M be the median through B and let $D = \frac{A+C}{2}$. If $|A-B|^2 = |B-C|^2$, then M is the perpendicular bisector of AC by Lemma 1.32(i). Therefore, den(BC,AC) = den(AC,AB) by Lemma 1.38.

If den(BC,AC) = den(AC,AB), then $r_M(B) = B$ and $r_M(A) = C$ (again by Lemmas 1.38, 1.32(i)). Since r_M is an isometry, $|A - B|^2 = |r_M(A) - r_M(B)|^2 = |C - B|^2$. $\square$

Corollary 1.40. *The $\triangle(A, B, C)$ is equilateral if and only if all its dengles are equal.*

Proposition 1.41.

i) *Let C be a circle centered at B, L a line and $p \in L \cap C$. Then $L \perp BP$ if and only if L is tangent to C.*

ii) *Let C, D be circles centered at A, B respectively. Let $p \in C \cap D$. Then den($T_p(C)$,$T_p(D)$) = den(AP,BP).*

Proof: i) Assume L is tangent to C. There is a unique line N through B and perpendicular to L. Let $Q \in L \cap N$. If $Q \neq P$, then $L = PQ$ and $R = 2Q - P \in L$. Since $\frac{P+R}{2} = Q \in N$, N is the perpendicular bisector of PR. Therefore, $r_N(P) = R$. But $B \in N$ and $p \in C \implies R = r_N(P) \in C$. This contradicts the fact that L is tangent to C. Thus, $P = Q$ and $(BP = N) \perp L$.

Conversely, assume $L \perp BP$. Suppose there exists $P \neq Q \in L \cap C$. Consider $\triangle BPQ$. Since $P, Q \in C$ and B is the center of B, $|P - B|^2 = |Q - B|^2$. Thus, $\triangle BPQ$ is isosceles and

$$den(BQ, PQ) = den(PQ, BP) = den(L, BP) = -1.$$

I.e., $BQ \perp L$. This gives two distinct lines BP, BQ passing through B and perpendicular to L, a contradiction. Thus, L is tangent to C.

ii) By part (i), $T_p(C) \perp AP$ and $T_p(D) \perp BP$. Thus, den(AP,BP) = den($T_p(C)$,$T_p(D)$) by Proposition 1.19. □

Proposition 1.42. *If char($\mathbb{F}$) $\neq 3$, then the medians of $\triangle ABC$ intersect at $\frac{A+B+C}{3}$ (called the* **centroid** *of $\triangle ABC$). If char($\mathbb{F}$) $= 3$, then the medians are (distinct) parallel lines.*

Proof: Assume char($\mathbb{F}$) $\neq 3$. Let M be the median passing through B and $\frac{A+C}{2}$. Then $M = \left(\frac{A+C}{2} - B\right)\mathbb{F} + B$ and thus $\frac{A+B+C}{3} = \frac{2}{3}\left(\frac{A+C}{2} - B\right) + B \in M$. By symmetry, $\frac{A+B+C}{3}$ lies on the other two medians as well.

If char($\mathbb{F}$) $= 3$, then $2 =$ -1 and thus

$$A - \frac{B+C}{2} = A + B + C = B - \frac{A+C}{2} = C - \frac{A+B}{2}.$$

Thus, the dengles between the medians $A\left(\frac{B+C}{2}\right)$, $B\left(\frac{A+C}{2}\right)$ and $C\left(\frac{B+C}{2}\right)$ are all one and they are all parallel. If $A\left(\frac{B+C}{2}\right) = C\left(\frac{A+B}{2}\right)$, then A, B, C are all collinear. Hence, $A\left(\frac{B+C}{2}\right) \neq C\left(\frac{A+B}{2}\right)$ and all three lines are distinct by symmetry. $\square$

Proposition 1.43.

i) *The perpendicular bisectors of the sides of a triangle are concurrent at the center (called the* **circumcenter***) of the circle (called the* **circumcircle***) passing through the vertices of the triangle.*

ii) *Let $P \neq Q$ be points on a circle C. The perpendicular bisector M of PQ passes through the center of C. Equivalently, when $M \cap C \neq 0$, PQ is parallel to the tangent lines at the intersections of M with C.*

Proof: i) Let P, Q, R be the vertices of the triangle and $D = a\mathbb{S} + b$ the unique circle through P, Q, R. Let L be the line through b and $\frac{P+Q}{2}$.

Since $|P-b|^2 = |Q-b|^2$ and $|P-\frac{P+Q}{2}|^2 = |Q-\frac{P+Q}{2}|^2$, we know $b\left(\frac{P+Q}{2}\right)$ is the perpendicular bisector of PQ by Lemma 1.32(i). So b lies on the perpendicular bisector of PQ and on the other two by symmetry.

ii) Choose $R \in C - \{P, Q\}$ and consider $\triangle PQR$. Then PQ is the side of a triangle and $B \in M$ where B is the center of C by i).

If $M \cap C \neq \emptyset$, let $W \in M \cap C$. Then $T_W(C) \perp BW$ by Prop. 1.41. Therefore by Lemma 1.9(iii),

$$PQ \parallel T_W(C) \iff PQ \perp BW \iff BW = M \iff B \in M.$$

(since M is the unique line containing W and perpendicular to PQ). $\square$

Proposition 1.44. *The three perpendiculars from the vertices to the opposite sides of a triangle meet at a point (called the* **orthocenter***).*

Proof: Let C be the circle through the vertices A, B, C of the triangle. WMA $C = \mathbb{S}$. Consider $M = (A + B + C)B$. Now

$$\begin{aligned} M \perp AC &\iff \frac{A - C}{(A + B + C) - B} \in \mathbb{I} - \{0\} \iff \frac{A - C}{A + C} \in \mathbb{I} - \{0\} \\ &\iff \frac{A - C}{A + C} = -\frac{(\overline{A} - \overline{C})}{\overline{A} + \overline{C}} \iff A\overline{A} - C\overline{C} = -A\overline{A} + C\overline{C} \iff A\overline{A} = C\overline{C}. \end{aligned}$$

But $A, C \in \mathbb{S} \implies A\overline{A} = C\overline{C} \implies M \perp AC$.

Thus, M is the perpendicular from the vertex B to AC and it contains $A + B + C$. By symmetry, $A + B + C$ lies on all three of the perpendiculars from the vertices to the opposite sides. $\square$

Lemma 1.45. *Assume $X \notin \triangle(A, B, C)$. Let Q, R be the intersection points of the perpendiculars from X to AB, AC respectively. Then the angle bisector L of den(AC,AB) at A exists and contains X if and only if $|X - Q|^2 = |X - R|^2$.*

Proof: Assume $X \in L$ and den(AR,L) = den(L,AQ). Since reflections conjugate dengles and r_L fixes L, we have

$$den(A(r_L(R)), L) = den(r_L(A)r_L(R), L) = \frac{1}{den(AR, L)} = \frac{1}{den(L, AQ)} = den(AQ, L).$$

Thus, $A(r_L(R))$ and AQ are both lines making the same dengle with L and we must therefore have $A(r_L(R)) = AQ$. So $r_L(R) \in AB$. Similarly, $RX \perp AR$ and $X \in L$ implies $(r_L(R))X \perp (A(r_L(R)) = AB)$. Since the unique line passing through X and perpendicular to AB is QX, we know $r_L(R) \in QX$. So $r_L(R) \in (AB) \cap (QX) = Q$. Consequently, $r_L(R) = Q$ and $|X - R|^2 = |X - r_L(R)|^2 = |X - Q|^2$.

Conversely, if $|X-Q|^2 = |X-R|^2$, then the Pythagorean Theorem gives that

$$|A - Q|^2 = |A - X|^2 - |Q - X|^2 = |A - X|^2 - |R - X|^2 = |A - R|^2.$$

Let

$$G = \{z \mid |z - X|^2 = |Q - X|^2\} \text{ and } H = \{z \mid |z - A|^2 = |Q - A|^2\}.$$

Then $\{Q, R\} = G \cap H$ since G and H are distinct circles. Therefore, $r_{AX}(R) \in G \cap H$ since r_{AX} preserves distance and fixes X, A. Since $R \notin AX$, we have $r_{AX}(R) = Q$. Thus,

$$den(AR, AX) = \frac{1}{den(A(r_{AX}(R)), AX)} = den(AX, AQ)$$

and AX bisects den(AR,AQ) = den(AC,AB) at A. $\square$

Remark: By Proposition 1.21, all the dengles of $\triangle ABC$ can be bisected if and only if all the dengles of $\triangle ABC$ are in $\mathbb{S}_+$.

Proposition 1.46.

i) *If all the dengles of $\triangle(A,B,C)$ are in $\mathbb{S}_+$, then the angle bisectors are concurrent (at a point called the* **incenter***).*

ii) *There is a unique circle (centered at the incenter and called the* **inscribed circle***) which is tangent to all the sides of $\triangle(A,B,C)$ if and only if the dengles of $\triangle(A,B,C)$ are in $\mathbb{S}_+$.*

Proof: i) Assume $\beta^2 = \text{den}(AB,BC)$, $\gamma^2 = \text{den}(BC,CA)$, $\tau^2 = \text{den}(CA,AB)$ $\in \mathbb{S}_+$.

Let L, M, N be the bisectors of β^2 at B, γ^2 at C, τ^2 at A respectively. Note that

$$den(L,M) = den(L,BC)den(BC,M) = \beta\gamma.$$

Now $\text{den}(L,M) = 1 \implies \tau^2 = \frac{1}{\beta^2\gamma^2} = 1$. Since A,B,C are noncollinear, we therefore know $\text{den}(L,M) \neq 1$ and there exists an $x \in L \cap M$. There exist unique points $P \in AC, Q \in AB, R \in BC$ such that $XP \perp AC, XQ \perp AB, XR \perp BC$. By Lemma 1.44, $X \in L \implies |X-Q|^2 = |X-R|^2$ and $X \in M \implies |X-P|^2 = |X-R|^2$. Thus, $|X-P|^2 = |X-Q|^2$ and $X \in N$ by Lemma 1.45 again. So L, M, N are concurrent at X.

ii) Moreover, since P, Q, R are all equidistant from X, all three points lie on the circle C centered at X of sqradius $|P-X|^2$. Since $AB \perp QX$, AB is tangent to C by Prop. 1.41(i). By symmetry, C is tangent to all three sides of $\triangle(A,B,C)$.

Conversely, if G is any circle centered at Y and tangent to all the sides of

$\triangle(A, B, C)$, then the angle bisectors must exist and be concurrent at Y by Prop. 1.41(i) and Lemma 1.45. Thus, all the dengles of $\triangle(A, B, C)$ are in $\mathbb{S}_{+}$.

This also shows the uniqueness of the C above since $Y = X$. $\square$

Definition: Two triangles $\triangle(A, B, C)$ and $\triangle(P, Q, R)$ are said to be **isometric** (denoted $\triangle(A, B, C) \cong \triangle(P, Q, R)$) if there exists a $g \in \mathrm{Isom}(\mathbb{E})$ such that $g(A) = P$, $g(B) = Q, g(C) = R$.

Remark: Since reflections are allowed and reflections conjugate dengles, g may not preserve the orientation of $\triangle(A, B, C)$ (just as in the classical case).

Proposition 1.47. *(SSS) If $|P - Q|^2 = |A - B|^2$, $|Q - R|^2 = |B - C|^2$ and $|R - P|^2 = |C - A|^2$, then $\triangle(A, B, C) \cong \triangle(P, Q, R)$.*

Proof: WMA that $B = Q = 0$ (by applying $z \mapsto z - Q$ to $\triangle(P, Q, R)$ and $z \mapsto z - B$ to $\triangle(A, B, C)$). Since $|P - 0|^2 = |A - 0|^2$, A and P both lie on the circle G centered at 0 of sqradius $|P|^2$. By Lemma 1.27, there is a rotation r with respect to G taking A to P. Applying r to $\triangle(A, 0, C)$, we now have $r(A) = P$, $r(0) = 0$, $r(C) = \widetilde{C}$. Now $|R - 0|^2 = |\widetilde{C} - 0|^2$ and $|R - P|^2 = |\widetilde{C} - P|^2 \implies R, \widetilde{C} \in H \cap K$ where $H = (R\overline{R})\mathbb{S}$ and $K = (|R - P|^2)\mathbb{S} + P$. By Lemma 1.32(ii), either $\widetilde{C} = R$ or $r_{OP}(\widetilde{C}) = R$. In either case, $\triangle(A, B, C) \cong \triangle(P, Q, R)$. $\square$

Lemma 1.48. *Let $B \neq C$, $Q \neq R \in \mathbb{E}$. Then $\tau^{-1} \circ \phi \in Isom(\mathbb{E})$ where $\phi, \tau \in B$ with $\phi(B) = 0 = \tau(Q)$ and $\phi(C) = 1 = \tau(R)$ iff $|B - C|^2 = |Q - R|^2$.*

Proof: Now

$$\phi(z) = \frac{z-B}{C-B} \text{ and } \tau(z) = \frac{z-Q}{R-Q}.$$

Thus,

$$\tau^{-1} \circ \phi(z) = [(R-Q)z + Q] \circ \frac{z-B}{C-B} = \left[\frac{R-Q}{C-B}\right] z + \left(Q - \frac{B(R-Q)}{C-B}\right).$$

So

$$\begin{aligned}
\tau^{-1} \circ \phi \in Isom(\mathbb{E}) \iff \frac{R-Q}{C-B} \in \mathbb{S} &\iff \left(\frac{R-Q}{C-B}\right)\left(\frac{\overline{R}-\overline{Q}}{\overline{C}-\overline{B}}\right) = 1 \\
&\iff (R-Q)(\overline{R-Q}) = (C-B)(\overline{C-B}) \\
&\iff |R-Q|^2 = |C-B|^2. \quad \square
\end{aligned}$$

Proposition 1.49. *(DSD)*

If den(AB,BC) = β = den(PQ,QR), den(BC,AC) = γ = den(QR,RP), and $|B-C|^2 = |Q-R|^2$, then $\triangle(A,B,C) \cong \triangle(P,Q,R)$.

Proof: Let $\phi, \tau \in B$ with $\phi(B) = 0 = \tau(Q), \phi(C) = 1 = \tau(R)$. Since ϕ and τ preserve dengles, we know

$$den(\phi(A)0, \mathbb{F}) = \beta = den(\tau(P)0, \mathbb{F}),$$

$$den(\mathbb{F}, \phi(A)1) = \gamma = den(\mathbb{F}, \tau(P)1).$$

Since there is a unique line making any specified dengle with $\mathbb{F}$ at 0, we must have that $\phi(A)0 = \tau(P)0$ and $\phi(A)1 = \tau(P)1$. Since $\phi(A)0$ and $\phi(A)1$ are distinct lines intersecting at $\phi(A)$ and $\tau(P)$, we have $\phi(A) = \tau(P)$. Thus, $\tau^{-1} \circ \phi(A) = P$, $\tau^{-1} \circ \phi(B) = Q$, and $\tau^{-1} \circ \phi(C) = R$. But $\tau^{-1} \circ \phi \in \text{Isom}(\mathbb{E})$ by Lemma 1.48. $\square$

Corollary 1.50. *(to the proof of DSD)*

i) *If den(AB,BC) = den(PQ,QR) in triangles* $\triangle(A,B,C)$ *and* $\triangle(P,Q,R)$*, then* $\phi(A)0 = \tau(P)0$ *where* $\phi, \tau \in B$ *with* $\phi(B) = 0 = \tau(Q)$*,* $\phi(C) = 1 = \tau(R)$*.*

ii) *If den(AB,BC) = den(PQ,QR) and den(BC,AC) = den(QR,RP), then there exists* $g \in B$ *with* $g(A) = P$*,* $g(B) = Q$*,* $g(C) = R$*.*

Proposition 1.51. *(DDS)*

If den(AB,BC) $= \beta =$ *den(PQ,QR), den(BC,AC)* $= \gamma =$ *den(QR,RP) and* $|A - C|^2 = |P - R|^2$*, then* $\triangle(A,B,C) \cong \triangle(P,Q,R)$*.*

Proof: Now den(AC,AB) $= \frac{1}{\beta\gamma} =$ den(PR,PQ). Since den(BC,AC) = den(QR,RP) and $|A - C|^2 = |P - R|^2$, the two triangles are isometric by DSD. □

Given a triangle $\triangle(P,Q,R)$, there is exactly one point $P \neq W \in PQ$ satisfying $|W - Q|^2 = |P - Q|^2$, namely $W = 2Q - P$.

Proposition 1.52. *(SDS) If den(AB,BC)* $= \beta =$ *den(PQ,QR),* $|A - B|^2 = |P - Q|^2$ *and* $|B - C|^2 = |Q - R|^2$*, then* $\triangle(A,B,C) \cong \triangle(P,Q,R)$ *or* $\triangle(A,B,C) \cong \triangle(2Q - P,Q,R)$*. If* $\beta = -1$*, then* $\triangle(A,B,C) \cong \triangle(P,Q,R)$*.*

Proof: By Corollary 1.50(i), we know $\phi(A)0 = \tau(P)0$ where $\phi, \tau \in B$ with $\phi(B) = 0 = \tau(Q)$, $\phi(C) = 1 = \tau(R)$. Since $|B - C|^2 = |Q - R|^2$, $\tau^{-1} \circ \phi$ is an isometry. Now $\phi(A) \in \tau(P)0 \implies \tau^{-1} \circ \phi(A) \in PQ$. But

$$|P - Q|^2 = |A - B|^2 = |\tau^{-1} \circ \phi(A) - \tau^{-1} \circ \phi(B)|^2 = |\tau^{-1} \circ \phi(A) - Q|^2.$$

There are exactly two points on PQ equidistant from Q, namely P and $2Q-P$. Thus, $\tau^{-1} \circ \phi(A) = P$ or $\tau^{-1} \circ \phi(A) = 2Q - P$. So $\tau^{-1} \circ \phi$ is an isometry from $\triangle(A, B, C)$ to $\triangle(P, Q, R)$ or $\triangle(2Q - P, Q, R)$. If $\beta = -1$, then QR is the perpendicular bisector of $P(2Q - P)$ and consequently $r_{QR}(2Q - P) = P$. If $\tau^{-1} \circ \phi(A) = 2Q - P$, then $r_{QR} \circ \tau^{-1} \circ \phi(A) = P$ and so $\triangle(A, B, C) \cong \triangle(2Q - P, Q, R) \cong \triangle(P, Q, R)$. $\square$

Definition: $\triangle(A, B, C)$ and $\triangle(P, Q, R)$ are **weakly isometric** (denoted $\cong_W$) if there exists a $g \in \mathrm{Isom}(\mathbb{E})$ such that $g(AB) = PQ$, $g(BC) = QR$ and $g(AC) = PR$.

In this terminology, the data for DSD gives that $\triangle(A, B, C) \cong_W \triangle(P, Q, R)$.

Proposition 1.53. *(DSS) Assume den(AB,BC) = β = den(PQ,QR), $|B - C|^2 = |Q - R|^2$ and $|A - C|^2 = |P - R|^2$. Then den(PR,QR) $\in \{\ \sigma =$ den$(AC, AB), \frac{1}{\sigma}\ \}$. If $\beta = -1$, then $\triangle(A, B, C) \cong_W \triangle(P, Q, R)$.*

Proof: By Corollary 1.50(i), $\phi(A)0 = \tau(P)0$ where $\phi, \tau \in B$ with $\phi(B) = 0 = \tau(Q)$, $\phi(C) = 1 = \tau(R)$. If $\phi(A) = \tau(P)$, then

$$den(PR, PQ) = den(\tau(P)1, \tau(P)0)$$

$$= den(\phi(A)1, \phi(A)0) = den(AC, AB) = \sigma.$$

Otherwise, $\triangle(1, \tau(P), \phi(A))$ is an isosceles triangle since $|A - C|^2 = |P - R|^2$. Thus,

$$den(PR, PQ) = den(\tau(P)1, \tau(P)\phi(A))$$

$$= den(\tau(P)\phi(A), \phi(A)1) = den(AB, AC) = \frac{1}{\sigma}.$$

If $\beta = -1$, then $\phi(A)0 = \tau(P)0 = \mathbb{I}$ since $\mathbb{I}$ is the unique line through 0 and perpendicular to $\mathbb{F}$. Since $|\tau(P) - 1|^2 = |\phi(A) - 1|^2$, $\phi(A), \tau(P) \in \mathbb{I} \cap G$ where G

is the circle centered at 1 of sqradius $|\tau(P)-1|^2$. But $\mathbb{I}\cap G = \{\tau(P), \overline{\tau(P)}\}$ by Lemmas 1.11(ii), 1.17(i). Thus, $\phi(A)=\tau(P)$ or $\phi(A)=\overline{\tau(P)}$. Since $|B-C|^2 = |Q-R|^2$, $\triangle(A,B,C) \cong_W \triangle(P,Q,R)$ by either $\tau^{-1}\circ\phi$ or $\overline{z}\circ\tau^{-1}\circ\phi$. $\square$

Remark: Consider the special case of the above proposition when $A = P$ and $C = R$. Now $\phi(z) = \dfrac{z-B}{C-B}$ and $\tau(z) = \dfrac{z-Q}{C-Q}$ so

$$\begin{aligned}
\phi(A) = \tau(P) = \tau(A) \iff\ & \frac{A-B}{C-B} = \frac{A-Q}{C-Q} \\
\iff\ & -BC - AQ + AB + CQ = 0 \\
\iff\ & (A-C)(B-Q) = 0 \iff B = Q.
\end{aligned}$$

Thus, if $\triangle(A,B,C) \neq \triangle(A,Q,C)$ then $\phi(A)\neq\tau(A)$ and we always have that den(AC,AQ) and den(AC,AB) are conjugate.

Theorem 1.54. *(Essential Uniqueness of Dengles)*

Let C be a circle centered at R and $p \notin C$, $p \neq R$. If Q and W are distinct points of C and den(PQ,QR) = den(PW,WR), then $r_{PR}(PQ) = PW$ and one of the following occurs:

i) $Q,\ W \in PR$

ii) *PQ, PW are both tangent to C and $r_{PR}(Q) = W$*

iii) $(PQ)\cap C = \{\ Q, r_{PR}(W)\ \}$, $(PW)\cap C = \{\ W, r_{PR}(Q)\ \}$ *and* $r_{PR}(Q) \neq W$.

Proof: Consider $\triangle(P,Q,R)$ and $\triangle(P,W,R)$. Since $|Q-R|^2 = |W-R|^2$, we know from the above remark that σ = den(PR,PQ) and den(PR,PW) are conjugate. But den(PR,$r_{PR}(PQ)$) = den($r_{PR}(PR), r_{PR}(PQ)$) = $\frac{1}{\sigma}$ also. Thus, $r_{PR}(PQ) = PW$ since both lines make dengle $\frac{1}{\sigma}$ with PR at P. Note that

$r_{PR}(C) = C$ since $R \in PR$. Thus, $Q \in (PQ) \cap C$ which implies that $r_{PR}(Q) \in (PW) \cap C$ and we have $r_{PR}(Q), W \in (PW) \cap C$.

Case 1. $r_{PR}(Q) = W$.

Then

$$\begin{aligned}\beta \;=\; den(PW, WR) \;=\; den(PQ, QR) &= \frac{1}{den(r_{PR}(PQ), r_{PR}(QR))} \\ &= \frac{1}{den(PW, WR))} = \frac{1}{\beta}\end{aligned}$$

and $\beta = \pm 1$. If $\beta = 1$, then $PQ \parallel QR$ and $PW \parallel WR$. Since $PQ = QR$ and $PW = WR$, we know $Q, W \in PR$. If $\beta = -1$, then $PQ \perp QR$ and $PW \perp WR$. Consequently, PQ and PW are both tangent to C.

Case 2. $r_{PR}(Q) \neq W$.

Then $(PW) \cap C = \{\ W,\ r_{PR}(Q)\ \}$. Applying r_{PR} to both sides of the equation gives $(PQ) \cap C = \{\ Q,\ r_{PR}(W)\ \}$. $\square$

Definition: The triangles $\triangle(A, B, C)$ and $\triangle(P, Q, R)$ are said to be **similar** (denoted $\triangle(A, B, C) \sim \triangle(P, Q, R)$) if there exists a $g \in B$ with $g(A) = P$, $g(B) = Q$, $g(C) = R$.

If $\triangle(A, B, C) \sim \triangle(P, Q, R)$, then $\dfrac{A-B}{C-B} = \dfrac{P-Q}{R-Q}$ and $\dfrac{A-C}{B-C} = \dfrac{P-R}{Q-R}$ since B preserves ratios. On the other hand, if $\dfrac{A-B}{C-B} = \dfrac{P-Q}{R-Q}$ and $\dfrac{A-C}{B-C} = \dfrac{P-R}{Q-R}$, then den($AB$,$BC$) = den($PQ$,$QR$) and den($BC$,$AC$) = den($QR$,$RP$). Then by Corollary 1.50(ii), we have

$$\begin{aligned}\triangle(A, B, C) \sim \triangle(P, Q, R) &\iff \frac{A-B}{C-B} = \frac{P-Q}{R-Q} \\ &\iff den(AB, BC) = den(PQ, QR) \text{ and } den(BC, AC) = den(QR, RP).\end{aligned}$$

Thus, B is the trig group of $\mathbb{E}$.

Consider $\triangle(A, B, C)$ where $\theta = \text{den}(AB, BC)$. We define

$$\cos^2(\theta) = \frac{(\theta+1)^2}{4\theta} = \frac{(\theta+\overline{\theta})+2}{4} \in \mathbb{F}.$$

From the definition of $\cos^2(\theta)$, we can derive the squares of the other trigonometric functions using the familiar identities that hold in the classical case. For example,

$$\sin^2(\theta) = 1 - \cos^2(\theta) = \frac{(\theta-1)^2}{-4\theta} = \frac{2-(\theta+\overline{\theta})}{4} \in \mathbb{F},$$
$$\tan^2(\theta) = \frac{\sin^2(\theta)}{\cos^2(\theta)} = \frac{-(\theta-1)^2}{(\theta+1)^2} \text{ when } \theta \neq -1.$$

We therefore have the following formulas:

1) $\cos^2(\theta) = \dfrac{(\theta+1)^2}{4\theta}$
2) $\sin^2(\theta) = \dfrac{(\theta-1)^2}{-4\theta}$
3) $i\tan(\theta) = \dfrac{\theta-1}{\theta+1} \in \mathbb{I}$ when $\theta \neq -1$
4) $i\sin(\theta)\cos(\theta) = \dfrac{\theta-\overline{\theta}}{4}$

Notation: In $\triangle(A, B, C)$, let $\alpha = \text{den}(CA, AB)$, $\beta = \text{den}(AB, BC)$, $\gamma = \text{den}(BC, CA)$ and $a = |B-C|^2$, $b = |A-C|^2$, $c = |A-B|^2$.

Proposition 1.55. *(Law of Sines)*

$$\frac{a^2}{\sin^2(\alpha)} = \frac{b^2}{\sin^2(\beta)} = \frac{c^2}{\sin^2(\gamma)}.$$

Proof: Since $\sin^2(\theta) = \frac{2-\theta-\overline{\theta}}{4}$, it suffices to show that

$$\frac{a^2}{2-\alpha-\overline{\alpha}} = \frac{b^2}{2-\beta-\overline{\beta}} = \frac{c^2}{2-\gamma-\overline{\gamma}}.$$

Since B preserves dengles and ratios (and $\frac{a^2}{2-\alpha-\overline{\alpha}} = \frac{b^2}{2-\beta-\overline{\beta}}$ is equivalent to $\frac{a^2}{b^2} = \frac{2-\alpha-\overline{\alpha}}{2-\beta-\overline{\beta}}$), we may assume $B = 1,\ C = 0$. Now $\gamma = \frac{A}{\overline{A}},\ \beta = \frac{\overline{A}-1}{A-1},\ \alpha = \frac{\overline{A}(A-1)}{A(\overline{A}-1)},\ a^2 = 1,\ b^2 = A\overline{A}$ and $c^2 = |A-1|^2 = (A-1)(\overline{A}-1)$. Thus,

$$2-\alpha-\overline{\alpha} = 2 - \frac{\overline{A}(A-1)}{A(\overline{A}-1)} - \frac{A(\overline{A}-1)}{\overline{A}(A-1)} = \frac{2A\overline{A} - \overline{A}^2 - A^2}{A\overline{A}(A-1)(\overline{A}-1)},$$
$$2-\beta-\overline{\beta} = 2 - \frac{\overline{A}-1}{A-1} - \frac{A-1}{\overline{A}-1} = \frac{2A\overline{A} - \overline{A}^2 - A^2}{(A-1)(\overline{A}-1)},$$
$$2-\gamma-\overline{\gamma} = 2 - \frac{A}{\overline{A}} - \frac{\overline{A}}{A} = \frac{2A\overline{A} - A^2 - \overline{A}^2}{A\overline{A}}.$$

Hence,

$$\frac{a^2}{2-\alpha-\overline{\alpha}} = \frac{A\overline{A}(A-1)(\overline{A}-1)}{2A\overline{A} - \overline{A}^2 - A^2} = \frac{b^2}{2-\beta-\overline{\beta}} = \frac{c^2}{2-\gamma-\overline{\gamma}}. \quad \square$$

Proposition 1.56. *(Law of Cosines)*

$$(a^2 + b^2 - c^2)^2 = 4a^2b^2\cos^2(\gamma).$$

Proof: Since $\cos^2(\gamma) = \dfrac{\gamma+\overline{\gamma}+2}{4}$, we want to show that

$$(a^2 + b^2 - c^2)^2 = a^2b^2(\gamma+\overline{\gamma}+2).$$

WMA $B = 0,\ C = 1$.Then $\gamma = \frac{A}{\overline{A}},\ c^2 = |A-1|^2 = A\overline{A} - A - \overline{A} + 1,\ b^2 = A\overline{A}$ and $a^2 = 1$. Thus,

$$a^2b^2(\gamma+\overline{\gamma}+2) = A\overline{A}(\frac{A}{\overline{A}} + \frac{\overline{A}}{A} + 2) = A^2 + \overline{A}^2 + 2A\overline{A},$$
$$(a^2+b^2-c^2)^2 = (1 + A\overline{A} - (A\overline{A} - A - \overline{A} + 1))^2 = (A+\overline{A})^2. \quad \square$$

Definition: In an isosceles triangle $\triangle(A,B,C)$ with $|A-B|^2 = |B-C|^2$, the **engle** from AB to BC (denoted en(AB,BC)) is $\dfrac{C-B}{A-B}$.

If $\triangle(P,Q,R) \sim \triangle(A,B,C)$, then en($PQ$,$QR$) = en($AB$,$BC$) since B preserves ratios.

Since $|A-B|^2 = |B-C|^2$, en(AB,BC) $\in \mathbb{S}$. Consequently,

$$den(AB,BC) = \frac{en(AB,BC)}{\overline{en(AB,BC)}} = (en(AB,BC))^2.$$

Moreover,

$$\left(\frac{\delta+\overline{\delta}}{2}\right)^2 = \frac{\delta^2+2\delta\overline{\delta}+\overline{\delta}^2}{4} = \frac{\theta+\overline{\theta}+2}{4} = \cos^2(\theta)$$

where θ = den(AB,BC) and δ = en(AB,BC).

Thus, for an isosceles triangle $\triangle(A,B,C)$ with $|A-B|^2 = |B-C|^2$, θ = den(AB,BC), δ = en(AB,BC), we define

$$\cos(\theta) = \frac{\delta+\overline{\delta}}{2}.$$

In this case, we also define $i\sin(\theta) = \dfrac{\delta-\overline{\delta}}{2}$.

Let $P \neq Q$ be points on a circle with center R. Since $|P-R|^2 = |Q-R|^2$, δ = en(PR,RQ) is defined.

Definition: Let $P_1, P_2, P_3, \ldots, P_n$ be distinct points, no three of which are collinear.

The union of the lines $P_1P_2, P_2P_3, \ldots, P_{n-1}P_n, P_nP_1$ is an n-**gon**, denoted $P_1P_2\cdots P_n$.

The points P_i are the **vertices** of the n-gon and the lines making up the n-gon are called **sides**.

The notation $(P_1, P_2, P_3, \ldots, P_n)$ will denote the n-gon with $\mathrm{den}(P_1P_2, P_2P_3)$, $\mathrm{den}(P_2P_3, P_3P_4)$, ... , $\mathrm{den}(P_{n-1}P_n, P_nP_1)$.

Note that the product of the dengles of $(P_1, P_2, P_3, \ldots, P_n)$ is one.

An n-gon with four sides is a **quadrilateral**, one with five sides is a **pentagon**, etc.

Proposition 1.57. *In $PQRS$, $S - P = R - Q$ if and only if $PQ \parallel RS$ and $PS \parallel QR$.*

Proof: If $S - P = R - Q$, then $Q - P = R - S$. Thus, $\frac{R-S}{Q-P} = 1 = \frac{R-Q}{S-P} \in \mathbb{F}$ and $PQ \parallel RS$, $PS \parallel QR$.

Conversely, assume $PQ \parallel RS$ and $PS \parallel QR$. Note that $S(S + Q - P) \parallel PQ$ since $\frac{Q-P}{(S+Q-P)-S} = 1$. Thus, $RS = S(S + Q - P)$ and $S + Q - P \in RS$. Analogously, $S+Q-P \in QR$. Since $QR \cap RS = \{R\}$, we have $R = S+Q-P$. $\square$

Definition: $PQRS$ is a **parallelogram** if $S - P = R - Q$. The **diagonals** of $PQRS$ are PR and QS.

Proposition 1.58. *$PQRS$ is a parallelogram if and only if the diagonals of $PQRS$ bisect each other.*

Proof: The diagonals PR and QS of $PQRS$ bisect each other if and only if $\frac{P+R}{2} = \frac{Q+S}{2} \iff P + R = Q + S \iff S - P = R - Q \iff PQRS$ is a parallelogram. $\square$

Proposition 1.59. *If $PQRS$ is a parallelogram, then*

$$2|Q - P|^2 + 2|R - Q|^2 = |R - P|^2 + |Q - S|^2.$$

Proof: Let $u = Q - P = R - S$, $v = R - Q = S - P$. Then $u + v = R - P$ and $u - v = Q - S$. But

$$|u+v|^2 + |u-v|^2 = (u+v)(\overline{u+v}) + (u-v)(\overline{u-v})$$
$$= 2u\overline{u} + 2v\overline{v} = 2|Q-P|^2 + 2|R-Q|^2. \quad \square$$

Proposition 1.60. *$PQRS$ is a parallelogram if and only if $|Q-P|^2 = |R-S|^2$, $|S-P|^2 = |R-Q|^2$ and $r_L(P) \neq R$ where L is the perpendicular bisector of QS.*

Proof: WMA $S = -1$ and $Q = 1$. Then $L = \mathbb{I}$ and $r_L(z) = -\overline{z}$. If $|1-P|^2 = |R+1|^2$ and $|P+1|^2 = |R-1|^2$, then $P\overline{P} - P - \overline{P} = R\overline{R} + R + \overline{R}$ and $P\overline{P} + P + \overline{P} = R\overline{R} - R - \overline{R}$. Adding these two equations gives $P\overline{P} = R\overline{R}$ and subtracting them gives $P + \overline{P} = -(R + \overline{R})$. Since $-P$, $-\overline{P}$ are the roots of $x^2 + (P+\overline{P})x + P\overline{P}$ and R is a root of $x^2 - (R+\overline{R})x + R\overline{R} = x^2 + (P+\overline{P})x + P\overline{P}$, we know $R = -P$ or $R = -\overline{P}$. But $r_L(P) = -\overline{P} \neq R$ so $R = -P$. Thus, $S - P = S + R = R - 1 = R - Q$ and $PQRS$ is a parallelogram.

Conversely, if $PQRS$ is a parallelogram, then $|1-P|^2 = |R+1|^2$ and $|P+1|^2 = |R-1|^2$. If $-\overline{P} = r_L(P) = R$, then $-1 - P = S - P = R - Q = -\overline{P} - 1$ and $P \in \mathbb{F}$. This can't happen since P, S, Q are not collinear. Thus, $r_L(P) \neq R$. $\square$

Remark: The condition that $r_L(P) \neq R$ is clearly necessary (see Figure 1.60.1).

Proposition 1.61. *If $PS \parallel QR$ and $|S-P|^2 = |R-Q|^2$ in $PQRS$, then either $PQRS$ or $PRQS$ is a parallelogram.*

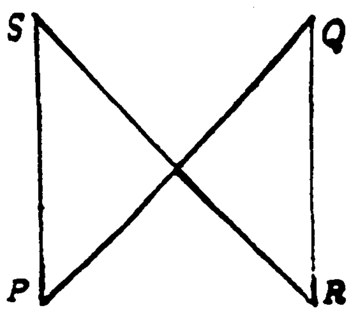

FIGURE 1.60.1

Proof: Let $z = \frac{R-Q}{S-P} \in \mathbb{F}^\times$ since $PS \parallel QR$. Now $|S-P|^2 = |R-Q|^2$ implies that $(S-P)(\overline{S-P}) = (R-Q)(\overline{R-Q}) \implies z\bar{z} = 1$ and $z \in \mathbb{S}$. Therefore, $z \in \mathbb{F}^\times \cap \mathbb{S} = \{\pm 1\}$. If $z = 1$, then $S-P = R-Q$ and $PQRS$ is a parallelogram. If $z = -1$, then $S-P = Q-R$ and $PRQS$ is a parallelogram. $\square$

In (P,Q,R,S), den(PQ,QR) and den(RS,SP) are said to be **opposite**; den(RS,SP) and den(SP,PQ) are said to be **adjacent**.

Proposition 1.62. *(P,Q,R,S) is a parallelogram if and only if both pairs of opposite dengles are equal and den(PQ,RS) $\neq -1$.*

Proof: If (P,Q,R,S) is a parallelogram, then den(PQ,RS) $= 1 \neq$ -1. Also

$$den(PQ, QR) = \rho\left(\frac{R-Q}{Q-P}\right) = \rho\left(\frac{S-P}{R-S}\right) = den(RS, SP),$$
$$den(QR, RS) = \rho\left(\frac{R-S}{R-Q}\right) = \rho\left(\frac{Q-P}{S-P}\right) = den(SP, PQ).$$

Conversely, assume $\rho\left(\frac{R-Q}{Q-P}\right) = \rho\left(\frac{S-P}{R-S}\right)$, $\rho\left(\frac{R-S}{R-Q}\right) = \rho\left(\frac{Q-P}{S-P}\right)$ and den(PQ,RS) $\neq$ -1. Then $\rho\left(\frac{R-Q}{S-P}\right) = \rho\left(\frac{Q-P}{R-S}\right)$ and $\rho\left(\frac{R-S}{Q-P}\right) =$

$\rho\left(\frac{R-Q}{S-P}\right)$. Thus, den($RS$,$PQ$) = den($PS$,$RQ$) = den($PQ$,$RS$). Consequently, den($PQ$,$RS$) = ± 1. Since den(PQ,RS) $\neq$ -1, $PQ \parallel RS$ and $PS \parallel RQ$. $\square$

Remark: The condition that den(PQ,RS) $\neq$ -1 is necessary in Proposition 1.62. Consider the construction of Figure 1.62.1 in the classical case. Now $\beta = \frac{\pi}{2} - \alpha = \gamma$ and $\tau = \pi + \alpha$. Since $e^{2i(\pi+\alpha)} = e^{2i\pi}e^{2i\alpha} = e^{2i\alpha}$, opposite pairs of dengles are equal but $PQRS$ is not a parallelogram.

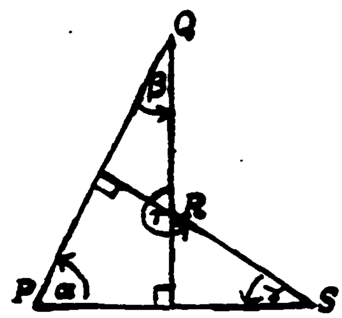

FIGURE 1.62.1

Proposition 1.63. *Let α = den(SP,PQ), β = den(PQ,QR) and γ = den(QR,RS) in (P,Q,R,S). Then (P,Q,R,S) is a parallelogram if and only if $\alpha\beta = 1 = \beta\gamma$.*

Proof: (P,Q,R,S) is a parallelogram if and only if

$$SP \parallel QR \text{ and } PQ \parallel RS \iff den(SP,QR) = 1 = den(PQ,RS) \iff \alpha\beta = 1 = \beta\gamma. \quad \square$$

Corollary 1.64. *If β = den(SP,PQ) = den(PQ,QR) in parallelogram (P,Q,R,S), then $\beta = -1$.*

Proof: By Proposition 1.63, $\beta^2 = 1$. If $\beta = 1$, then $SP = PQ$ and S, P, Q are collinear. Thus, $\beta = -1$. $\square$

Definition: (P, Q, R, S) is a **rectangle** if all four of its dengles are equal and den(PQ,RS) $\neq -1$. $PQRS$ is a **rhombus** if all four sides have equal length.

By Proposition 1.62 and Corollary 1.64, a rectangle is a parallelogram with all dengles equal to -1.

Lemma 1.65. *A rhombus $PQRS$ is a parallelogram.*

Proof: By Proposition 1.60, it suffices to show that $r_L(P) \neq R$ where L is the perpendicular bisector of QS. WMA $S = -1$, $Q = 1$. Then $L = \mathbb{I}$ and $r_L(z) = -z$. Since $|1 - P|^2 = |R + 1|^2 = |P + 1|^2$, we have $P\overline{P} - P - \overline{P} = R\overline{R} + R + \overline{R} = P\overline{P} + P + \overline{P}$ and thus $P = -\overline{P}$. Then $r_L(P) = -\overline{P} = P \neq R$. $\square$

Proposition 1.66.

i) *The diagonals of a rectangle (P, Q, R, S) have equal length.*

ii) *The diagonals of a rhombus $PQRS$ are perpendicular.*

Proof: i) Since $|S - P|^2 = |R - Q|^2$, $\triangle(P, S, R) \cong \triangle(Q, R, S)$ by SDS. Thus, $|R - P|^2 = |S - Q|^2$.

ii) Let $\{T\} = QS \cap PR$. By Propositions 1.58 and 1.59,

$$4|Q-P|^2 = |R-P|^2 + |Q-S|^2 = |2(P-T)|^2 + |2(Q-T)|^2 = 4(|P-T|^2 + |Q-T|^2).$$

Since $|Q-P|^2 = |P-T|^2 + |Q-T|^2$, $QT \perp PT$ by the Pythagorean Theorem. $\square$

Definition: A **trapezoid** is a quadrilateral with exactly one pair of parallel sides.

Proposition 1.67. *If $PQRS$ is a trapezoid with $PS \parallel QR$, then*

$$\left|\frac{P+Q}{2} - \frac{R+S}{2}\right|^2 = \frac{|P-S|^2 + |R-Q|^2 + 2(P-S)(\overline{Q-R})}{4}.$$

Proof:

$$\begin{aligned}
|P+Q-R-S|^2 &= (P+Q-R-S)(\overline{P}+\overline{Q}-\overline{R}-\overline{S}) \\
&= (P\overline{P} - P\overline{S} - \overline{P}S + S\overline{S}) + (R\overline{R} - Q\overline{R} - \& \,\overline{Q}R + Q\overline{Q}) \\
&\qquad + (P\overline{Q} - S\overline{Q} - P\overline{R} + \overline{R}S) + (\overline{P}Q - Q\overline{S} - \overline{P}R + R\overline{S}) \\
&= |P-S|^2 + |R-Q|^2 + (P-S)(\overline{Q-R}) + (\overline{P-S})(Q-R).
\end{aligned}$$

But $(P-S)(\overline{Q-R}) = (\overline{P-S})(Q-R)$ since $PS \parallel QR$. $\square$

Let $D \in \mathbb{E}$, L a side of $\triangle(A,B,C)$.

Definition: The intersection of L with the perpendicular from D to L is called the **foot** of the perpendicular.

Theorem 1.68. *(The Nine-Point Circle)*

Let σ be the orthocenter, τ the circumcenter and G the circumcircle of $\triangle(A,B,C)$. Then the following nine points all lie on the circle H centered at $\frac{\sigma+\tau}{2}$ with $sqr(H)=\frac{sqr(G)}{4}$:

i) $\frac{A+B}{2}, \frac{B+C}{2}, \frac{A+C}{2}$

ii) $\frac{\sigma+A}{2}, \frac{\sigma+B}{2}, \frac{\sigma+C}{2}$

iii) *The feet of the three perpendiculars from A to BC, B to AC, C to AB.*

Proof: WMA $G = \mathbb{S}$ so that $A,\ B,\ C \in \mathbb{S}$ and $\tau = 0$. Then H has center $\frac{\sigma}{2}$ and sqradius $\frac{1}{4}$. From the proof of Proposition 1.44, we know $\sigma = A+B+C$.

Thus,

$$\left|\frac{\sigma}{2}-\frac{A+B}{2}\right|^2=\left|\frac{C}{2}\right|^2=\frac{1}{4} \text{ and } \left|\frac{\sigma+A}{2}-\frac{\sigma}{2}\right|^2=\left|\frac{A}{2}\right|^2=\frac{1}{4}.$$

Let λ be the foot of the perpendicular from A to BC. Then $\lambda \in BC$, $\lambda A \perp BC$ and $\sigma \in \lambda A$. Let $\mu := \frac{-BC}{A}$. Now

$$den(\mu A, BC)=\left(\frac{A(B-C)}{-BC-A^2}\right)\left(\frac{-\overline{BC}-\overline{A}^2}{\overline{A}(\overline{B}-\overline{C})}\right)=\frac{-AC+A\overline{B}-\overline{A}B+\overline{A}C}{-\overline{A}C-A\overline{B}+\overline{A}B+A\overline{C}}=-1.$$

Since λA is the unique line through A and perpendicular to BC, $\mu A=\lambda A$. Thus, $(B\lambda = BC) \perp (\mu\sigma=\lambda A)$. Since $|\sigma-B|^2=|A+C|^2=|\mu-B|^2$, $\triangle(\mu,B,\lambda)\cong\triangle(\sigma,B,\lambda)$ by DSS. Consequently, $|\mu-\lambda|^2=|\sigma-\lambda|^2$ and $\lambda=\dfrac{\sigma+\mu}{2}$ since λ, μ, σ are collinear. Then $\left|\dfrac{\sigma+\mu}{2}-\dfrac{\sigma}{2}\right|^2=\left|\dfrac{\mu}{2}\right|^2=\left|\dfrac{BC}{2A}\right|^2=\dfrac{1}{4}$ and $\lambda\in H$. By symmetry, the other six points also lie on H. □

H is called the **nine-point circle of the triangle.**

The line passing through the orthocenter, circumcenter, centroid (if char($\mathbb{F}$) $\neq 3$) and center of the nine-point circle is called the **Euler line** of the triangle. (If A, B, $C \in \mathbb{S}$ as above, the four points are $A+B+C$, 0, $\dfrac{A+B+C}{3}$, $\dfrac{A+B+C}{2}$ respectively which are clearly collinear.)

Let z_1,z_2,z_3,z_4 be distinct points of $\mathbb{S}$. The nine-point circles of $\triangle(z_2z_3z_4)$, $\triangle(z_1z_3z_4)$, $\triangle(z_1z_2z_4)$ and $\triangle(z_1z_3z_4)$ are centered at $P_1=\dfrac{z_1+z_3+z_4}{2}$, $P_2=\dfrac{z_1+z_3+z_4}{2}$, $P_3=\dfrac{z_1+z_2+z_4}{2}$ and $P_4=\dfrac{z_1+z_2+z_3}{2}$ respectively and all have sqradius $\frac{1}{4}$. Thus, P_1, P_2, P_3, P_4 all lie on the circle centered at $\dfrac{z_1+z_2+z_3+z_4}{2}$ with sqradius $\frac{1}{4}$, called the **nine-point circle of the quadrilateral** $z_1z_2z_3z_4$.

Given five distinct points $z_1, z_2, z_3, z_4, z_5 \in \mathbb{S}$, **the nine-point circle of the pentagon** $z_1z_2z_3z_4z_5$ is the circle centered at $\dfrac{z_1+z_2+z_3+z_4+z_5}{2}$ with sqradius $\frac{1}{4}$ and contains the centers of the nine point circles of the quadrilaterals $z_2z_3z_4z_5$, $z_1z_3z_4z_5$, $z_1z_2z_3z_5$, $z_1z_2z_3z_4$.

There is such a result for each n-gon. The classical version of this infinite sequence of theorems is due to J.L. Coolidge.

Theorem 1.69. *The three perpendiculars from the midpoints of the sides of a triangle to the tangents to the circumcircle at the opposite vertices meet at the center of the nine-point circle of the triangle.*

Proof: WMA that the circumcircle of $\triangle(ABC)$ is $\mathbb{S}$. Then the center of the nine-point circle is $\frac{\sigma}{2}$ where $\sigma = A+B+C$. Let M be the perpendicular from $\dfrac{A+B}{2}$ to the tangent line L of $\mathbb{S}$ at C. Now $\left(\frac{\sigma}{2}\right)\left(\frac{A+B}{2}\right) \parallel (0C)$ since $\dfrac{C-0}{\frac{\sigma}{2}-\frac{A+B}{2}} = \dfrac{2C}{C} = 2 \in \mathbb{F}$. Since $0C \perp L$, $\left(\frac{\sigma}{2}\right)\left(\frac{A+B}{2}\right) \perp L$. Thus, $\left(\frac{\sigma}{2}\right)\left(\frac{A+B}{2}\right) = M$ and $\frac{\sigma}{2} \in M$. By symmetry, the three perpendiculars are concurrent at $\frac{\sigma}{2}$. □

Definition: The **centroid** of m distinct points $P_1, P_2, \ldots, P_m$ is $\dfrac{P_1+P_2+\cdots+P_m}{m}$ when char($\mathbb{F}$) $\neq m$.

Theorem 1.70. *Assume char($\mathbb{F}$) $\neq n-1$. Let n distinct points lie on a circle. From the centroid of $n-1$ of these points, drop a perpendicular to the tangent to the circle at the remaining point. These n perpendiculars are concurrent.*

Proof: WMA the circle is $\mathbb{S}$. Let $\tau = P_1 + P_2 + \cdots + P_n$. Let M be the perpendicular from $\frac{\tau - P_n}{n-1}$ to the tangent line L to $\mathbb{S}$ at P_n. Note that

$(\frac{\tau}{n-1})(\frac{\tau-P_n}{n-1}) \parallel (0P_n)$ since $\left(\dfrac{P_n}{\frac{\tau}{n-1}-\frac{\tau-P_n}{n-1}}\right) = n-1 \in \mathbb{F}$. Since $0P_n \perp L$, we have $(\frac{\tau}{n-1})(\frac{\tau-P_n}{n-1}) \perp L$ and $\frac{\tau}{n-1} \in M$. $\square$

The classical version of Theorems 1.69 and 1.70 is due to M.B. Cantor. We will see more of these infinite sequences of theorems in the next section.

2. Conformal Geometry.

We now consider the action of $PGL_2(\mathbb{E})$ on $\mathbb{P}^1_{\mathbb{E}} = \mathbb{E} \cup \{\infty\}$.

Lemma 2.1. *$PGL_2(\mathbb{E}) = \left\langle \mathbb{E}^{\times} z + \mathbb{E},\ \frac{-1}{z} \right\rangle$ and $PSL_2(\mathbb{E}) = < \mathbb{E}_{+} z + \mathbb{E},\ \frac{-1}{z} >$.*

Proof: Let $g(z) = \dfrac{az+b}{cz+d} \in PGL_2(\mathbb{E})$ (respectively $PSL_2(E)$). If $c = 0$, then $g(z) \in PGL_2(\mathbb{E})_\infty = \mathbb{E}^{\times} z + \mathbb{E}$ (respectively $PSL_2(\mathbb{E})_\infty = \mathbb{E}_{+} z + \mathbb{E}$). If $c \neq 0$, then $g(z) = \dfrac{az+b}{cz+d} = \dfrac{a}{c} - \dfrac{ad-bc}{c^2 z + cd} = (z \mapsto (ad-bc)z + \frac{a}{c}) \circ (\frac{-1}{z}) \circ (z \mapsto c^2 z + cd)$ is in $< \mathbb{E}^{\times} z + \mathbb{E},\ \frac{-1}{z} >$ (respectively $< \mathbb{E}_{+} z + \mathbb{E},\ \frac{-1}{z} >$). $\square$

Remark: Note that the action of $PGL_2(\mathbb{F})$ on $\mathbb{P}^1_{\mathbb{E}}$ commutes with conjugation. That is, if $g \in PGL_2(\mathbb{E})$, then $g \circ \overline{z} = \overline{z} \circ g$.

Definition: An **extended line** in $\mathbb{P}^1_{\mathbb{E}}$ is $L \cup \{\infty\}$, denoted $\widehat{L}$, where L is a line in $\mathbb{E}$.

A **mirror** is a Euclidean circle or an extended line.

Lemma 2.2. *$PGL_2(\mathbb{E})_{\widehat{\mathbb{F}}} = PGL_2(\mathbb{F})$.*

Proof: Clearly, $PGL_2(\mathbb{F}) \subseteq PGL_2(\mathbb{E})_{\widehat{\mathbb{F}}}$. Let $g(z) = \frac{az+b}{cz+d} \in PGL_2(\mathbb{E})_{\widehat{\mathbb{F}}}$. Then for all $z \in \widehat{\mathbb{F}}$,

$$\begin{aligned} \frac{az+b}{cz+d} &= \frac{\overline{a}z+\overline{b}}{\overline{c}z+\overline{d}} \\ &\Longrightarrow (az+b)(\overline{c}z+\overline{d}) = (\overline{a}z+\overline{b})(cz+d) \\ &\Longrightarrow a\overline{c}z^2 + (b\overline{c}+a\overline{d})z + b\overline{d} = \overline{a}cz^2 + (\overline{a}d - \overline{b}c)z + \overline{b}d \\ &\Longrightarrow a\overline{c},\ b\overline{d} \in \mathbb{F} \text{ and } b\overline{c} + a\overline{d} = \overline{a}d - \overline{b}c. \end{aligned}$$

If $d = 0$, then $b\bar{c} \in \mathbb{F}$. Also $c \neq 0$ since $\det(g) = ad - bc \neq 0$. Therefore,

$$g(z) = \frac{az+b}{cz+d} = \frac{a\bar{c}z + b\bar{c}}{c\bar{c}z + \bar{c}d} \in PGL_2(\mathbb{F}).$$

A similar argument works if $a = 0$, $b = 0$, or $c = 0$. Thus, we may assume $a,\ b,\ c,\ d \in \mathbb{E}^\times$. Since $\frac{a}{\bar{a}} = \frac{c}{\bar{c}}$, $\frac{b}{\bar{b}} = \frac{d}{\bar{d}}$ and $b\bar{c} + a\bar{d} = \bar{a}d - \bar{b}c$, we have

$$\begin{aligned} \frac{cd}{\bar{c}\bar{d}}\left(b\bar{c} + a\bar{d}\right) &= \frac{ab}{\bar{a}\bar{b}}\left(\bar{a}d + \bar{b}c\right) \\ \Longrightarrow bc\left(\frac{d}{\bar{d}} - \frac{a}{\bar{a}}\right) &= ad\left(\frac{b}{\bar{b}} - \frac{c}{\bar{c}}\right) \\ \Longrightarrow (ad - bc)\left(\frac{b}{\bar{b}} - \frac{c}{\bar{c}}\right) &= 0 \Longrightarrow \frac{b}{\bar{b}} = \frac{c}{\bar{c}}. \end{aligned}$$

Thus, $\frac{a}{\bar{a}} = \frac{c}{\bar{c}} = \frac{c}{\bar{c}} = \frac{d}{\bar{d}}$. In particular, $\bar{a}b,\ \bar{a}d \in \mathbb{F}$ and $g(z) = \frac{az+b}{cz+d} = \frac{a\bar{a}z + \bar{a}b}{\bar{a}cz + \bar{a}d}$ is in $PGL_2(\mathbb{F})$. $\square$

Lemma 2.3. *The $PGL_2(\mathbb{E})$ orbit of $\widehat{\mathbb{F}}$ contains all mirrors.*

Proof: Since $B \subseteq PGL_2(\mathbb{E})$ acts transitively on lines and fixes ∞, clearly all extended lines are contained in the $PGL_2(\mathbb{E})$ orbit of $\widehat{\mathbb{F}}$. Since B also acts transitively on circles, it suffices to note that $g(\mathbb{S}) = \widehat{\mathbb{I}}$ where $g(z) = \frac{z-1}{z+1} \in PGL_2(\mathbb{E})$. $\square$

Lemma 2.4. *$g(\widehat{\mathbb{F}})$ is a mirror for $g \in PGL_2(\mathbb{E})$.*

Proof: Let $T^{-1} \in PGL_2(\mathbb{E})$ and $T(z) = \frac{az+b}{cz+d}$. Now $T^{-1}\left(\frac{a}{c}\right) = \infty$, $T^{-1}(\infty) = \frac{-d}{c}$.

Now $w \in T^{-1}(\mathbb{F}) \iff T(w) \in \mathbb{F} \iff \frac{aw+b}{cw+d} = \overline{\frac{aw+b}{cw+d}}$

$$\iff (a\bar{c} - \bar{a}c)|w|^2 + (a\bar{d} - \bar{b}c)w + (-\bar{a}d + b\bar{c})\bar{w} + (b\bar{d} - \bar{b}d) = 0$$

since $w \neq \dfrac{-d}{c}$. If $\dfrac{a}{c} \in \mathbb{F}$, then $w \in T^{-1}(\mathbb{F})$ if and only if $\lambda(\overline{w-k}) = \overline{\lambda}(w-k)$ where $\lambda = b\overline{c} - \overline{a}d$ and $k = \dfrac{-b\overline{d}}{\overline{\lambda}}$. But

$$\lambda\mathbb{F} + k = \{ \ x \in \mathbb{E} \mid \lambda(\overline{x-k}) = \overline{\lambda}(x-k) \ \} = T^{-1}(\mathbb{F} - \frac{a}{c}) \cup \{ \ \frac{-d}{c} = T^{-1}(\infty) \ \}.$$

Since $T^{-1}\left(\dfrac{a}{c}\right) = \infty$, $T^{-1}(\widehat{\mathbb{F}}) = \widehat{\lambda\mathbb{F}+k}$. If $\dfrac{a}{c} \notin \mathbb{F}$, then $w \in T^{-1}(\mathbb{F})$ if and only if

$$|w|^2 + \left(\frac{a\overline{d} - \overline{b}c}{a\overline{c} - \overline{a}c}\right) w + \left(\frac{-\overline{a}d + b\overline{c}}{a\overline{c} - \overline{a}c}\right) \overline{w} + \left(\frac{b\overline{d} - \overline{b}d}{a\overline{c} - \overline{a}c}\right) = 0.$$

Letting $\mu = \dfrac{ad - bc}{a\overline{c} - \overline{a}c}$ and $m = \dfrac{\overline{a}d - b\overline{c}}{a\overline{c} - \overline{a}c}$, we see that

$$\begin{aligned}\mu\mathbb{S} + m = \{ \ x \in \mathbb{E} \mid |x-m|^2 = |\lambda|^2 \ \} &= \{ \ x \in \mathbb{E} \mid x\overline{x} - \overline{m}x - m\overline{x} + m\overline{m} = \mu\overline{\mu} \ \} \\ &= T^{-1}(\mathbb{F}) \cup \{ \ \frac{-d}{c} = T^{-1}(\infty) \ \} \\ &= T^{-1}(\widehat{\mathbb{F}}). \quad \square\end{aligned}$$

Definition Let z_1, z_2, z_3, z_4 be distinct points in $\widehat{\mathbb{E}}$. The **cross-ratio** of z_1, z_2, z_3, z_4, denoted (z_1, z_2, z_3, z_4) is $S(z_1)$ where S is the unique element of $PGL_2(\mathbb{E})$ such that $S(z_2) = 1$, $S(z_3) = 0$, $S(z_4) = \infty$.

Theorem 2.5. *The $PGL_2(\mathbb{E})$ orbit of $\widehat{\mathbb{F}}$ is the set of all mirrors.*

Proof: Let C be a mirror and $T \in PGL_2(\mathbb{E})$. Let z_1, z_2, z_3, $z_4 \in C$ be distinct and $(z_1, z_2, z_3, z_4) = S(z_1)$. Then $S^{-1}(\widehat{\mathbb{F}})$ is a mirror containing z_2, z_3, z_4 by Lemma 2.4. Since three distinct points determine a unique mirror, $C = S^{-1}(\widehat{\mathbb{F}})$. Thus, $T(C) = T \circ S^{-1}(\widehat{\mathbb{F}})$ is a mirror by Lemma 2.3. The result now follows from Lemma 2.3. $\square$

Lemma 2.6. *The cross-ratio is invariant under $PGL_2(\mathbb{E})$.*

Proof: Let $T \in PGL_2(\mathbb{E})$. Assume $S \in PGL_2(\mathbb{E})$ with $S(z_2) = 1$, $S(z_3) = 0$, and $S(z_4) = \infty$. Then $S \circ T^{-1}(T(z_2)) = 1$, $S \circ T^{-1}(T(z_3)) = 0$, $S \circ T^{-1}(T(z_4)) = \infty$. Therefore, $(T(z_1), T(z_2), T(z_3), T(z_4)) = S \circ T^{-1}(T(z_1)) = S(z_1) = (z_1, z_2, z_3, z_4)$. $\square$

Propostion 2.7. *Let z_1, z_2, z_3, z_4 be distinct points in $\widehat{\mathbb{E}}$. The cross-ratio $(z_1, z_2, z_3, z_4) \in \mathbb{F}$ if and only if z_1, z_2, z_3, z_4 lie on a mirror.*

Proof: Let $(z_1, z_2, z_3, z_4) = S(z_1)$. Then $S^{-1}(\widehat{\mathbb{F}})$ is a mirror containing z_2, z_3, z_4 by Lemma 2.3. If z_1, z_2, z_3, $z_4 \in C$ where C is a mirror, then $C = S^{-1}(\widehat{\mathbb{F}})$. Then since $z_4 = S^{-1}(\infty)$ and $z_4 \neq z_1 \in S^{-1}(\widehat{\mathbb{F}})$, we have $(z_1, z_2, z_3, z_4) = S(z_1) \in \mathbb{F}$. Conversely, if $S(z_1) \in \mathbb{F}$, then $S^{-1}(\widehat{\mathbb{F}})$ is a mirror containing z_1, z_2, z_3, z_4. $\square$

The map $g : \mathbb{S} \mapsto \widehat{\mathbb{I}}$ given by $g(z) = \dfrac{z-1}{z+1}$ defined in the proof of Lemma 2.3 is a useful tool. The following illustrates some of its applications to number theory.

Applications

1) Find all Pythagorean triples, i.e., all (a, b, c) such that a, b, c are positive integers satisfying $a^2 + b^2 = c^2$.

Solution: Since (ka, kb, kc) is a Pythagorean triple for any Pythagorean triple (a, b, c) and positive integer k, we may assume a, b, c have no common divisor. Since $c \neq 0$, $a^2 + b^2 = c^2 \iff \left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$. Thus, the problem can equivalently be phrased as follows:

Find all $x + iy \in \mathbb{Q}(i)$ lying in the first quadrant of $\mathbb{S}$ and with $x, y \in \mathbb{Q}$ in reduced form.

Now $(h = g^{-1}) : \widehat{\mathbb{I}} \mapsto \mathbb{S}$ is given by $h(z) = \dfrac{1+z}{1-z}$. In particular, the set $W = \{\, ir \mid 0 < r < 1,\ r \text{ a positive rational} \,\}$ maps onto the first quadrant of $\mathbb{S}$. So let $ri \in W$. Then $r = \dfrac{p}{q}$ where $q > p > 0,\ (p,q) = 1$. Then

$$h(ri) = \frac{1+ir}{1-ir} = \frac{1+2ir-r^2}{1+r^2} = \frac{q^2-p^2}{q^2+p^2} + i\frac{2pq}{q^2+p^2}.$$

Thus, the Pythagorean triples are of the form $(q^2 - p^2, 2pq, q^2 + p^2)$ where $q > p > 0$ and $\dfrac{q^2-p^2}{q^2+p^2}, \dfrac{2pq}{q^2+p^2}$ are in reduced form. If $d|(q^2 - p^2)$ and $d|(q^2 + p^2)$, then $d|2q^2$ and $d|2p^2$ (the sum and difference of $q^2 - p^2, q^2 + p^2$). Since $(p,q) = 1$, $d = 2$. But $q^2 - p^2, q^2 + p^2$ are both even if and only if p, q are both odd since $(p,q) = 1$. A similar argument shows that $\left(pq, \dfrac{q^2+p^2}{2}\right) = 1$ if p, q are both odd and $(2pq, q^2 + p^2) = 1$ otherwise. Hence the Pythagorean triples are of the form $\left(\dfrac{q^2-p^2}{2}, pq, \dfrac{q^2+p^2}{2}\right)$ for $q > p > 0,\ p, q$ both odd and $(q^2 - p^2, 2pq, q^2 + p^2),\ q > p > 0,\ p, q$ not both odd. $\square$

The above can be generalized as follows.

2) Find all positive integers (a, b, c) such that $a^2 + \lambda b^2 = c^2$ where λ is a positive square-free integer.

Solution: We want to find all $x + i\sqrt{\lambda}y \in \mathbb{Q}(i\sqrt{\lambda})$ lying in the first quadrant of $\mathbb{S}$ and with $x, y \in \mathbb{Q}$ in reduced form. With $W = \{\, i\sqrt{\lambda}r \mid 0 < r < 1,\ r \text{ a positive rational} \,\}$, we argue as in 1) to see that all solutions are of the form $(q^2 - \lambda p^2, 2pq, q^2 + \lambda p^2)$ where $q > \sqrt{\lambda}p > 0$ and

$\dfrac{q^2 - \lambda p^2}{q^2 + \lambda p^2}, \dfrac{2pq}{q^2 + \lambda p^2}$ are in reduced form. Let $\beta = gcd(q, \lambda)$. The solutions are thus of the form $\left(\dfrac{q^2 - \lambda p^2}{2\beta}, \dfrac{pq}{\beta}, \dfrac{q^2 + \lambda p^2}{2\beta}\right)$ when p, q, λ are all odd and $\left(\dfrac{q^2 - \lambda p^2}{\beta}, \dfrac{2pq}{\beta}, \dfrac{q^2 + \lambda p^2}{\beta}\right)$ otherwise where $q > \sqrt{\lambda}p > 0$.

3) Find all positive integers (a, b, c) such that $a^2 - \lambda b^2 = c^2$ where λ is a positive square-free integer.

Solution: We want to find all $x + \sqrt{\lambda}y \in \mathbb{Q}(\sqrt{\lambda})$ lying in the first quadrant of $\mathbb{S}$ and with $x, y \in \mathbb{Q}$ in reduced form. With $W = \{\ \sqrt{\lambda}r \mid 0 < r < 1,\ r \text{ a positive rational}\ \}$, we argue as in 1) to see that all solutions are of the form $(q^2 + \lambda p^2, 2pq, q^2 - \lambda p^2)$ where $q > \sqrt{\lambda}p > 0$ and $\dfrac{q^2 + \lambda p^2}{q^2 - \lambda p^2}, \dfrac{2pq}{q^2 - \lambda p^2}$ are in reduced form. Consequently, (a, b, c) is a solution to $a^2 - \lambda b^2 = c^2$ if and only if (c, b, a) is a solution to $a^2 + \lambda b^2 = c^2$.

Definition Let C, D be mirrors with $C \cap D = \{\ P, Q\ \}$. Choose an element $g \in PGL_2(\mathbb{E})$ with $g(P) = \infty$ and $g(C) = \widehat{\mathbb{F}}$. The **dengle from** C **to** D **at** Q is defined to be the dengle from $\mathbb{F}$ to $g(D) - \{\infty\}$ and is denoted den(C,D,Q).

Lemma 2.8. *The den(C,D,Q) is well-defined and is a $PGL_2(\mathbb{E})$ invariant.*

Proof: Assume $g, h \in PGL_2(\mathbb{E})$ with $g(C) = \widehat{\mathbb{F}} = h(C)$ and $g(P) = \infty = h(P)$. Since B acts transitively on $\mathbb{E}$, there exists $k \in B$ with $k(g \circ h^{-1}(0)) = 0, k(g \circ h^{-1}(1)) = 1$. Since $k \circ g$ and h agree on the three distinct points $h^{-1}(0), h^{-1}(1), \infty$, we know $h = k \circ g$. Let $X \neq Y \in D - \{P\}$. Since $k \in B$,

$$\begin{aligned} den(\mathbb{F}, h(D) - \{\infty\}) &= den(\mathbb{F}, k \circ g(D) - \{\infty\}) = \frac{k \circ g(X) - k \circ g(Y)}{\overline{k \circ g(X)} - \overline{k \circ g(Y)}} \\ &= \frac{g(X) - g(Y)}{\overline{g(X)} - \overline{g(Y)}} = den(\mathbb{F}, g(D) - \{\infty\}). \end{aligned}$$

Thus, den(C,D,Q) is well-defined.

Let $T \in PGL_2(\mathbb{E})$ and $X \neq Y \in C - \{P\}$. Let g and h be in $PGL_2(\mathbb{E})$ with $g(X) = 0 = h(T(X))$, $g(Y) = 1 = h(T(1))$, $g(P) = \infty = h(T(P))$. Then

$$\begin{aligned} den(C, D, Q) &= den(\mathbb{F}, g(D) - \{\infty\}) = den(\mathbb{F}, h \circ T(D) - \{\infty\}) \\ &= den(T(C), T(D), T(Q)). \quad \square \end{aligned}$$

Remark:

i) Distinct mirrors C, D are tangent if and only if $C \cap D = \{Q\}$ if and only if den(C,D,Q) $= 1$.

ii) If $Q \in L \cap M$ where L, M are lines, then den($\widehat{L}$,$\widehat{M}$,Q) $=$ den(L,M). (Since $P = \infty$ is the other intersection point of $\widehat{L}$ and $\widehat{M}$, den($\widehat{L}$,$\widehat{M}$,Q) $=$ den($g(L)$,$g(M)$) where $g \in PGL_2(\mathbb{E})_\infty = B$.)

Lemma 2.9. *If P and Q are the intersection points of mirrors C and D, then den(C,D,Q) $= \overline{den(C, D, P)}$.*

Proof: Let $R \in C - \{P, Q\}$, $W \in D - \{P, Q\}$. Let g be an element of $PGL_2(\mathbb{E})$ satisfying $g(P) = 0, g(Q) = \infty, g(R) = 1$. Then $h = \frac{1}{g} \in PGL_2(\mathbb{E})$ satisfies $g(Q) = 0$, $g(P) = \infty$, $g(R) = 1$. Thus,

$$\begin{aligned} den(C, D, P) &= den(\mathbb{F}, g(D) - \{\infty\}) = \frac{g(W)}{\overline{g(W)}} = \frac{\overline{h(W)}}{h(W)} \\ &= \overline{den(\mathbb{F}, h(D) - \{\infty\})} = \overline{den(C, D, Q)}. \quad \square \end{aligned}$$

Proposition 2.10. *Let L be a line and C, D be mirrors.*

i) *If $C \cap D = \{P, Q\}$ and $L \cap C = \{P\}$, then den(C,D,P) $=$ den($\widehat{L}$,D,P).*

ii) *If* $P \in L \cap C$ *and* C *is a Euclidean circle with center* A*, then* $den(C,\widehat{L},P)$ $= den(\ T_P(C),L) = -den(AP,L)$.

iii) *Let* $P \in C \cap D$ *and* C, D *be Euclidean circles centered at* A, B *respectively. Then* $den(C,D,P) = den(\ T_P(C),T_P(D)) = den(AP,BP)$.

Proof: i) By Lemma 2.8, we may assume that $P = \infty$, $Q = 0$ and $C = \widehat{\mathbb{F}}$. Then den(C,D,Q) = den$(\ \widehat{\mathbb{F}},D,Q)$ = den$(\ \widehat{L},D,X)$ where $\infty \neq X \in L \cap D$ by Proposition 1.18. Thus,

$$den(C,D,P) = \overline{den(C,D,Q)} = \overline{den(\ \widehat{L},D,X)} = den(\ \widehat{L},D,P).$$

ii) By i), den$(C,\widehat{L},P)$ = den$(\widehat{T_P(C)},\widehat{L},P)$ = den$(T_P(C),L)$. By Proposition 1.41(i), $T_P(C) \perp AP$. Thus,

$$den(AP,L) = den(AP,T_P(C))den(T_P(C),L) = -den(T_P(C),L).$$

iii) By i) and ii),

$$\begin{aligned} den(C,D,P) &= den(\widehat{T_P(C)},D,P) = \overline{den(D,\widehat{T_P(C)},P)} \\ &= \overline{den(T_P(D),T_P(C))} = den(T_P(C),T_P(D)). \end{aligned}$$

By Proposition 1.41(ii), den$(T_P(C),T_P(D))$ = den(AP,BP). □

Definition: The **reflection** about the mirror C is $g\overline{z}g^{-1}$ where $g \in PGL_2(\mathbb{E})$ and $g(\widehat{\mathbb{F}}) = C$.

Remarks:

i) Since $PGL_2(\mathbb{E})_{\widehat{\mathbb{F}}} = PGL_2(\mathbb{F})$ and $PGL_2(\mathbb{F})$ commutes with conjugation, reflections are well-defined: If $g\widehat{\mathbb{F}} = h\widehat{\mathbb{F}}$, then $f = g^{-1}h \in PGL_2(\mathbb{E})_{\widehat{\mathbb{F}}} = PGL_2(\mathbb{F})$. Thus, $g\overline{z}h^{-1} = (gf)\overline{z}(f^{-1}g^{-1}) = g\overline{z}(ff^{-1})g^{-1} = g\overline{z}g^{-1}$.

ii) If L is a line, then $r_L(z) = g\bar{z}g^{-1}$ where $g \in B \subseteq PGL_2(\mathbb{E})$ and $g(\mathbb{F}) = L$. Therefore, the reflection about $\overline{L}$ is r_L. If C is a Euclidean circle, then $r_C(z) = h \circ (\frac{1}{\bar{z}}) \circ h^{-1}$ where $h \in B$, $h(\mathbb{S}) = C$. Let $Q \in \mathbb{S} - \{\pm 1\}$. Then $k(\widehat{\mathbb{F}}) = \mathbb{S}$ where $k^{-1}(z) = \left(\frac{Q-1}{Q+1}\right)\left(\frac{z+1}{z-1}\right)$. It's easy to check that $\frac{1}{\bar{z}} = k \circ \bar{z} \circ k^{-1}$. Thus, $r_C(z) = h \circ (\frac{1}{\bar{z}}) \circ h^{-1} = (hk) \circ \bar{z} \circ (hk)^{-1}$ where $hk(\widehat{\mathbb{F}}) = C$. Hence, this definition of reflection about C agrees with our Euclidean definition and will be denoted r_C.

iii) Since the dengle between two mirrors is a dengle between two lines (after a change of coordinates), reflections invert dengles.

iv) If $g \in PGL_2(\mathbb{E})$, then $r_C = g^{-1} \circ r_{g(C)} \circ g$. (Let $h \in PGL_2(\mathbb{E})$ be such that $h(\widehat{\mathbb{F}}) = g(C)$. Then

$$g^{-1} \circ r_{g(C)} \circ g = g^{-1} \circ (h\bar{z}h^{-1}) \circ g = (g^{-1}h) \circ \bar{z} \circ (g^{-1}h)^{-1} = r_C$$

since $(g^{-1}h)(\widehat{\mathbb{F}}) = C$.)

Let W be the set of all mirrors in $\mathbb{P}^1_{\mathbb{E}}$ (i.e., the $PGL_2(\mathbb{E})$ orbit of $\widehat{\mathbb{F}}$).

Definition: A bijection $\phi : \mathbb{P}^1_{\mathbb{E}} \mapsto \mathbb{P}^1_{\mathbb{E}}$ is **conformal** if $\phi(W) = W$ and ϕ preserves dengles.

The set of all conformal maps forms a group under composition, denoted $\mathrm{Conf}(\mathbb{P}^1_{\mathbb{E}})$.

Lemma 2.11. *Let G be a group acting on the set X. If $H \leq G$ acts transitively on X and $H_x = G_x$ for some $x \in X$, then $H = G$.*

Proof: Let $g \in G$. Since H acts transitively on X, there exists $h \in H$ such that $h(x) = g(x)$. Then $h^{-1}g \in G_x = H_x$ and $g = h(h^{-1}g) \in HH_x = H$. $\Box$

Theorem 2.12. *Conf(* $\mathbb{P}^1_{\mathbb{E}}$ *)* $= PGL_2(\mathbb{E})$.

Proof: Clearly, $PGL_2(\mathbb{E}) \leq \mathrm{Conf}(\mathbb{P}^1_{\mathbb{E}})$. Now $\mathrm{Conf}(\mathbb{P}^1_{\mathbb{E}})$ acts on the set X of all triples (x, y, z) of elements of $\mathbb{P}^1_{\mathbb{E}}$ and $PGL_2(\mathbb{E})$ acts transitively on X. By Lemma 2.11, if $Conf(\mathbb{P}^1_{\mathbb{E}})_{(0,1,\infty)} = 1$ ($= PGL_2(\mathbb{E})_{(0,1,\infty)}$), then $PGL_2(\mathbb{E})$ $= \mathrm{Conf}(\mathbb{P}^1_{\mathbb{E}})$. Let $\tau \in Conf(\mathbb{P}^1_{\mathbb{E}})_{(0,1,\infty)}$ Let $P \in \mathbb{E} - \mathbb{F}$. Since τ fixes $0, 1, \infty$ and sends circles to circles, $\tau(\mathbb{F}) = \mathbb{F}$. Since den($\mathbb{F}$, $0P$) = den($\mathbb{F}$, $0\tau(P)$), $0P = 0\tau(P)$ and thus $\tau(P) \in 0P$. Similarly, $\tau(P) \in 1P$. Since $P \notin \mathbb{F}$, $0P \neq 1P$ and therefore $\{P\} = (0P) \cap (1P)$. Thus, $\tau(P) = P$ for every $P \in \mathbb{E} - \mathbb{F}$.

Let $Q \in \mathbb{F}$. Now $L = \mathbb{I} + Q$ is perpendicular to $\mathbb{F}$ at Q. Let $\alpha \in \mathbb{I} - \{0\}$. Then $\alpha + Q \in L - \mathbb{F}$ so $\tau(\alpha + Q) = \alpha + Q$. Since $\tau(L)$ is perpendicular to $\mathbb{F}$ and contains $\alpha + Q$, $\tau(L) = L$. Thus, $\tau(Q) \in \mathbb{F} \cap L = \{Q\}$. Hence, $\tau = 1$. $\Box$

It follows from Theorem 2.12 that the group of bijections of $\mathbb{P}^1_{\mathbb{E}}$ that either preserve dengles or invert dengles is $< PGL_2(\mathbb{E}), \overline{z} >$. For if $\phi \in \mathrm{Conf}(\mathbb{P}^1_{\mathbb{E}})$ inverts dengles, then $g = \phi \circ \overline{z}$ preserves dengles.

Proposition 2.13. *If* $\mathbb{F}^\times \subseteq \mathbb{E}_+$*, then the subgroup of* $< PGL_2(\mathbb{E}), \overline{z} >$ *generated by reflections is contained in* $< PSL_2(\mathbb{E}), \overline{z} >$.

Proof: Let $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in PGL_2(\mathbb{E})$. Then $g^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. Since $\overline{z} \circ g^{-1} = \overline{g^{-1}} \circ \overline{z}$, we have

$$g \circ \overline{z} \circ g^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \overline{d} & -\overline{b} \\ -\overline{c} & \overline{a} \end{bmatrix} \circ \overline{z} = \begin{bmatrix} a\overline{d}-b\overline{c} & -a\overline{b}+\overline{a}b \\ c\overline{d}-\overline{c}d & \overline{a}d-\overline{b}c \end{bmatrix} \circ \overline{z}.$$

Note that $-a\bar{b}+\bar{a}b,\ c\bar{d}-\bar{c}d \in \mathbb{I}$ and thus $(-a\bar{b}+\bar{a}b)(c\bar{d}-\bar{c}d) \in \mathbb{F}$. Therefore, $0 \neq \det(\overline{gg^{-1}}) = (a\bar{d}-b\bar{c})(\overline{a\bar{d}-b\bar{c}}) - (-a\bar{b}+\bar{a}b)(c\bar{d}-\bar{c}d) \in \mathbb{F}^{\times} \subsetneq \mathbb{E}_{+}$ and we have $\overline{gg^{-1}} \circ \bar{z} \ \in < PSL_2(\mathbb{E}), \bar{z} >$. □

Definition: If C, D are two mirrors with $P \in C \cap D$, then C and D are **perpendicular** (denoted $C \perp D$) if and only if den(C,D,P) $= -1$.

Proposition 2.14. *Let C, D be distinct mirrors with $P \in C \cap D$.*

i) *$C \perp D$ if and only if $r_C(D) = D$ (if and only if $r_D(C) = C$).*

ii) *If D is an extended line and C is a Euclidean circle with center Q, then $C \perp D$ if and only if $Q \in D$.*

Proof: i) Let $g \in PGL_2(\mathbb{E})$ such that $g(P) = \infty$ and $g(D) = \widehat{\mathbb{F}}$. Then $g(C) = \widehat{L}$ for some line L. Therefore,

$$r_C(D) = D \iff g^{-1} \circ r_{g(C)} \circ g(D) = D \iff r_{g(C)}(\widehat{\mathbb{F}}) = \widehat{\mathbb{F}} \iff r_L(\mathbb{F}) = \mathbb{F}$$
$$\iff L \perp \mathbb{F} \iff \widehat{L} \perp \widehat{\mathbb{F}} \iff g^{-1}(\widehat{L}) \perp g^{-1}(\widehat{\mathbb{F}}) \iff C \perp D.$$

ii) $C \perp D \iff r_D(C) = C \iff Q \in D$ by Lemma 1.25(ii). □

Definition: Mirrors C and D are said to be **orthogonal** (denoted $C \ \Psi \ D$) if and only if $r_C \circ r_D$ has order two.

Proposition 2.15. *Let C, D be distinct mirrors. The following are equivalent:*

i) $C \ \Psi \ D$

ii) *r_C and r_D commute*

iii) $r_D(C) = C$.

Proof: i) $\iff$ ii):

$$r_D \circ r_C = r_C \circ r_D \iff r_C(r_D \circ r_C)r_D = r_C(r_C \circ r_D)r_D = 1 \iff (r_C \circ r_D)^2 = 1.$$

ii) $\iff$ iii): Since $r_C \circ r_D$ and $r_D \circ r_C$ are both elements of $PGL_2(\mathbb{E})$,

$$r_C \circ r_D = r_D \circ r_C \iff r_C \circ r_D(z) = r_D \circ r_C(z) \text{ for all } z \in C.$$

But $r_C \circ r_D(z) = r_D \circ r_C(z)$ for all $z \in C$ iff $r_C \circ r_D(z) = r_D(z)$ for all $z \in C$ iff $r_D(z) \in C$ for all $z \in C$ iff $r_D(C) = C$. $\square$

Remark: If C, D are distinct mirrors with $C \cap D \neq \emptyset$, then $C \perp D$ if and only if $r_D(C) = C$ if and only if $C \ \Psi \ D$.

Proposition 2.16. *Let $C = a\mathbb{S} + b$ and $D = c\mathbb{S} + d$ be distinct. $C \ \Psi \ D$ if and only if $a\bar{a} + c\bar{c} = |b - d|^2$.*

Proof: First assume that $b = 0$. Let $\lambda = a\bar{a}$, $\mu = c\bar{c}$. $C \ \Psi \ D$ iff $(r_C \circ r_D)^2(z) = z$ for all $z \in \mathbb{P}^1_{\mathbb{E}}$. Now

$$r_C(z) = \frac{\lambda}{\bar{z}}, \quad r_D(z) = \frac{\mu}{\bar{z} - \bar{d}} + d.$$

Thus,

$$\begin{aligned}
r_C \circ r_D(z) &= \frac{\lambda}{\left(\frac{\mu}{z-d} + \bar{d}\right)} = \frac{\lambda(z-d)}{\bar{d}z + (\mu - d\bar{d})}, \\
(r_C \circ r_D)^2(z) &= \frac{\lambda\left[\frac{\lambda(z-d)}{\bar{d}z+(\mu-d\bar{d})}\right] - \lambda d}{\bar{d}\left[\frac{\lambda(z-d)}{\bar{d}z+(\mu-d\bar{d})}\right] + (\mu - d\bar{d})} = \frac{\lambda^2(z-d) - \lambda d(\bar{d}z + (\mu - d\bar{d}))}{\bar{d}\lambda(z-d) + (\mu - d\bar{d})(\bar{d}z + (\mu - d\bar{d}))} \\
&= \frac{(\lambda^2 - \lambda d\bar{d})z + (\lambda d^2\bar{d} - \lambda^2 d - \lambda d\mu)}{(\lambda\bar{d} + \mu\bar{d} - d\bar{d}^2)z + (\mu^2 - \lambda d\bar{d} - 2\mu d\bar{d} + d^2\bar{d}^2)}.
\end{aligned}$$

Assume $C \ \Psi \ D$. Then, in particular, $(r_C \circ r_D)^2(0) = 0$. Therefore,

$$\lambda d^2\bar{d} - \lambda^2 d - \lambda d\mu = \lambda d(d\bar{d} - \lambda - \mu) = 0.$$

Since $\lambda \neq 0$, we have $d = 0$ or $d\bar{d} = \lambda + \mu$. If $d = 0$, then $(r_C \circ r_D)^2(z) = \left(\frac{\lambda^2}{\mu^2}\right) z$ and thus $(r_C \circ r_D)^2(1) = 1$ gives $\lambda^2 = \mu^2$. Since $C \neq D$, $\lambda = -\mu$ and so $\lambda + \mu = 0 = d\bar{d}$ as above.

Conversely, if $\lambda + \mu = d\bar{d}$, then

$$\begin{aligned}
(r_C \circ r_D)^2(0) &= \frac{\lambda d(d\bar{d} - \lambda - \mu)}{\mu(\mu - d\bar{d}) + d\bar{d}(d\bar{d} - \lambda - \mu)} = \frac{0}{\mu(\mu - d\bar{d})} = 0, \\
(r_C \circ r_D)^2(\infty) &= \frac{\lambda(\lambda - d\bar{d})}{-\bar{d}(d\bar{d} - \lambda - \mu)} = \frac{\lambda(\lambda - d\bar{d})}{0} = \infty, \\
(r_C \circ r_D)^2(1) &= \frac{\lambda(\lambda - d\bar{d})}{\mu(\mu - d\bar{d})} = \frac{-\lambda\mu}{-\lambda\mu} = 1.
\end{aligned}$$

Since $(r_C \circ r_D)^2 \in PGL_2(\mathbb{E})$ and fixes three distinct points, $(r_C \circ r_D)^2 = 1$. Thus, $C \ \Psi \ D$ if and only if $\lambda + \mu = |d|^2$ when $b = 0$. If $b \neq 0$, consider $g(C)$ and $g(D)$ where $g(z) = z - b$. Since $g(C)$ has center 0, sqradius λ and $g(D)$ has center $g(d) = d - b$, sqradius μ, the above result gives $C \ \Psi \ D$ iff $\lambda + \mu = |b - d|^2$. $\square$

Definition Points $w_1, w_2, \ldots, w_n \in \mathbb{P}^1_{\mathbb{E}}$ are **cocyclic** if there is a mirror in $\mathbb{P}^1_{\mathbb{E}}$ containing all of them.

Lemma 2.17. *Let C_1, C_2, C_3, C_4 be mirrors in $\mathbb{P}^1_{\mathbb{E}}$ such that $C_1 \cap C_2 = \{z_1, w_1\}$, $C_2 \cap C_3 = \{z_2, w_2\}$, $C_3 \cap C_4 = \{z_3, w_3\}$, $C_4 \cap C_1 = \{z_4, w_4\}$ and $z_1, z_2, z_3, z_4, w_1, w_2, w_3, w_4$ are all distinct. Then z_1, z_2, z_3, z_4 are cocyclic if and only if w_1, w_2, w_3, w_4 are cocyclic.*

Proof: We may assume all of the mirrors are Euclidean circles. (Choose a point Q not lying on any of the C_i and conjugate it to ∞). Let

$$\begin{aligned} R_1 &= (z_4, w_1, z_1, w_4) = \left[\frac{z_4 - z_1}{z_4 - w_4}\right]\left[\frac{w_1 - w_4}{w_1 - z_1}\right], \\ R_2 &= (z_1, w_2, z_2, w_1) = \left[\frac{z_1 - z_2}{z_1 - w_1}\right]\left[\frac{w_2 - w_1}{w_2 - z_2}\right], \\ R_3 &= (z_2, w_3, z_3, w_2) = \left[\frac{z_2 - z_3}{z_2 - w_2}\right]\left[\frac{w_3 - w_2}{w_3 - z_3}\right], \\ R_4 &= (z_3, w_4, z_4, w_3) = \left[\frac{z_3 - z_4}{z_3 - w_3}\right]\left[\frac{w_4 - w_3}{w_4 - z_4}\right]. \end{aligned}$$

Note that $R_1 \in \mathbb{F}^\times$ since $z_1, w_1, z_4, w_4 \in C_1$. Similarly, $R_2, R_3, R_4 \in \mathbb{F}^\times$ and thus $\frac{R_2R_4}{R_1R_3} \in \mathbb{F}^\times$. But

$$\begin{aligned} \frac{R_2R_4}{R_1R_3} &= \left[\frac{z_1 - z_3}{z_1 - z_4}\right]\left[\frac{z_2 - z_4}{z_2 - z_3}\right]\left[\frac{w_1 - w_3}{w_1 - w_4}\right]\left[\frac{w_2 - w_4}{w_2 - w_3}\right] \\ &= (z_1, z_3, z_2, z_4)(w_2, w_4, w_1, w_3). \end{aligned}$$

Thus, $(z_1, z_3, z_2, z_4) \in \mathbb{F}$ if and only if $(w_2, w_4, w_1, w_3) \in \mathbb{F}$. $\square$

Definition: We say n lines are in **general position** if no two are parallel and no three meet at a point.

The intersection of two nonparallel lines is their **Clifford point**.

Given three lines in general position, we obtain $\binom{3}{2} = 3$ Clifford points. The (Euclidean) circle through these three points is the **Clifford circle**.

Lemma 2.18. *Let B, C, J, K be distinct points of $\mathbb{E}$, G the circle through B, C, J centered at P and H the circle through D, J, K centered at Q. If $BK = DK$, $CK = JK$ and $PK = QK$, then $BC \parallel DJ$.*

Proof: We may assume $B = -1$, $K = 1$, $C \in \mathbb{S}$. So $g = \mathbb{S}$ and $P = 0$. Since $D1 = \mathbb{F}$ and $Q1 = \mathbb{F}$, $D, Q \in \mathbb{F}$. Since $D, J, K \in H$, $|D - Q|^2 = |J - Q|^2 = |1 - Q|^2$. Therefore, $D^2 - 2DQ = J\overline{J} - (J + \overline{J})Q = 1 - 2Q$.

Since $C1 = J1$, $J \in (C-1)\mathbb{F}+1$. So $J = Ct - t + 1$, $t \in \mathbb{F}$. Therefore, $J\overline{J} = Xt^2 - Xt + 1$ and $J + \overline{J} = -Xt + 2$ where $X = 2 - C - \overline{C}$. Thus,

$$D^2 - 2DQ = 1 - 2Q = Xt^2 + XtQ - Xt + 1 - 2Q.$$

Since $D^2 - 2DQ = 1 - 2Q$, we have $D^2 - 2QD + (2Q-1) = 0$ and thus $D = 2Q - 1$.

Now $0 = Xt^2 + XtQ - Xt = Xt(t + Q - 1)$ and thus $t = 1 - Q$ ($X = 0 \implies C = 1$ and $t = 0 \implies J = 1$) and $J = C - CQ + Q$. Since $C \in \mathbb{S}$,

$$den(\ (-1)C\ ,\ DJ\ ) = \frac{(D-J)(\overline{C}+1)}{C+1)(D-\overline{J})} = \frac{(CQ+Q-C-1)(\overline{C}+1)}{(\overline{C}Q+Q-\overline{C}-1)(C+1)} = 1. \quad \square$$

Theorem 2.19.

i) *Let L_1, L_2, L_3, L_4 be lines in general position. The $\binom{4}{3} = 4$ Clifford circles of the triples $\{\ L_i, L_j, L_k \mid 1 \le i < j < k \le 4\ \}$ intersect at a point (the* **Clifford point** *of L_1, L_2, L_3, L_4).*

ii) *Let L_1, L_2, L_3, L_4, L_5 be lines in general position. The $\binom{5}{4} = 5$ Clifford points of the quadruples $\{\ L_i, L_j, L_k, L_m \mid 1 \le i < j < k < m \le 5\ \}$ are cocyclic (on the* **Clifford circle** *of L_1, L_2, L_3, L_4, L_5).*

Proof: i) Let $\{z_{jk}\} = L_j \cap L_k$, $1 \le j < k \le 4$ and C_{lmn} be the circle through z_{lm}, z_{mn}, z_{ln}. By Lemma 2.18, den(C_{134},C_{234}) $\neq 1$ and thus there exists a point $z_{34} \neq z \in C_{134} \cap C_{234}$. Now

$$\begin{aligned} \widehat{L_1} \cap \widehat{L_2} &= \{z_{12}, \infty\}, & \widehat{L_1} \cap C_{134} &= \{z_{13}, z_{14}\}, \\ \widehat{L_2} \cap C_{234} &= \{z_{23}, z_{24}\}, & C_{134} \cap C_{234} &= \{z_{34}, z\}. \end{aligned}$$

Since $\infty, z_{13}, z_{23}, z_{34} \in \widehat{L_3}$, we know from Lemma 2.17 that $z_{12}, z_{14}, z_{24}, z$ are also cocyclic. Thus, z is in C_{124}, the unique circle containing z_{12}, z_{14}, and z_{24}. Similarly, we know $\infty, z_{14}, z_{24}, z_{34} \in \widehat{L_4}$ and thus $z \in C_{123}$. Hence, $z \in C_{123} \cap C_{124} \cap C_{134} \cap C_{234}$.

ii) Define z_{ij}, C_{ijk} as in i) for $1 \leq i < j < k \leq 5$. Let z_{klmn} be a point in $C_{klm} \cap C_{lmn} \cap C_{kmn} \cap C_{kln}$ where $1 \leq k < l < m < n \leq 5$. Now $C_{123} \cap C_{125} = \{z_{12}, z_{1235}\}$, $C_{124} \cap C_{134} = \{z_{14}, z_{1234}\}$, $C_{125} \cap C_{145} = \{z_{15}, z_{1245}\}$, and $C_{134} \cap C_{135} = \{z_{13}, z_{1345}\}$. Also $z_{12}, z_{14}, z_{15}, z_{13} \in \widehat{L_1}$. If $|\{ z_{1235}, z_{1234}, z_{1245}, z_{1345} \}| < 4$, then $z_{1235}, z_{1234}, z_{1245}, z_{1345}$ are cocyclic. Otherwise, they are cocyclic by Lemma 2.17. A similar argument shows that any four of $z_{1234}, z_{1235}, z_{1245}, z_{1345}, z_{2345}$ are cocyclic. Hence, all five are cocyclic. □

Given lines $L_1, L_2, L_3, L_4, L_5, L_6$ in general position, the 6 Clifford circles of the quintuples $\{ L_i, L_j, L_k, L_m, L_n \mid 1 \leq i < j < k < m < n \leq 6 \}$ intersect at a point (the Clifford point of $L_1, L_2, L_3, L_4, L_5, L_6$). These results are part of an infinite sequence of theorems by W.K. Clifford.

Theorem 2.20. *Let $D \in \mathbb{E}$ and P, Q, R be the feet of the perpendiculars from D to BC, AC, AB respectively in $\triangle(ABC)$. Then P, Q, R are collinear if and only if D is on the circumcircle of $\triangle(ABC)$.*

Proof: If $D = C$, then $C = P = Q$ and the result holds. Thus, we may assume $D \notin \{A, B, C\}$. Since $DP \perp PB$ and $DR \perp RB$,

$$\left[\frac{P-B}{P-D}\right]\left[\frac{\overline{P}-\overline{D}}{\overline{P}-\overline{B}}\right]\left[\frac{R-D}{R-B}\right]\left[\frac{\overline{R}-\overline{B}}{\overline{R}-\overline{D}}\right] = den(DP, PB)den(RB, DR) = 1.$$

Thus, $(P,R,B,D) = \left[\frac{P-B}{P-D}\right]\left[\frac{R-D}{R-B}\right] \in \mathbb{F}$ and P,R,B,D lie on a mirror G in $\mathbb{P}^1_{\mathbb{E}}$. Similarly, P,Q,C,D lie on a mirror H in $\mathbb{P}^1_{\mathbb{E}}$ since $DP \perp PC$ and $DQ \perp QC$.

Now $G \cap AB = \{B,R\}$, $H \cap AC = \{C,Q\}$, $G \cap H = \{D,P\}$, and $AB \cap AC = \{A,\infty\}$. By Lemma 2.17, P,Q,R are collinear iff P,Q,R,∞ are cocyclic iff A,B,C,D are cocylic iff D lies on the circumcircle of $\triangle(ABC)$. □

When P,Q,R are collinear, the line through them is the **Simson line** of D with respect to $\triangle(ABC)$.

Lemma 2.21. *Assume the circumcircle of $\triangle(ABC)$ is $\mathbb{S}$, $D \in \mathbb{S} - \{A,B,C\}$ and P,Q,R are the feet of the perpendiculars from D to BC, AC, AB respectively. Then the equation of the Simson line of D with respect to $\triangle(ABC)$ is $Dz - \sigma_3\overline{z} = \frac{1}{2}(D^2 + \sigma_1 D - \sigma_2 - \frac{\sigma_3}{D})$ where $\sigma_1 = A+B+C$, $\sigma_2 = AB+AC+BC$, $\sigma_3 = ABC$.*

Proof: Since $D \notin \{A,B,C\}$, $P \neq Q$. Thus, the Simson line is PQ and its equation is $(\overline{P-Q})z - (P-Q)\overline{z} = \overline{P}Q - P\overline{Q}$. From the proof of Theorem 1.68, $2P = D + B + C - \frac{BC}{D}$ and $2Q = D + A + C - \frac{AC}{D}$. Thus,

$$\begin{aligned}(\overline{P-Q})z - (P-Q)\overline{z} &= \frac{(\overline{C-D})(\overline{A-B})}{2\overline{D}}\, z - \frac{(C-D)(A-B)}{2D}\, \overline{z} \\ &= \frac{D}{2}\left[\frac{(D-C)(B-A)}{ABCD}\right] z - \frac{(C-D)(A-B)}{2D}\, \overline{z}.\end{aligned}$$

$$
\begin{aligned}
4(\overline{P}Q - P\overline{Q}) &= (\overline{D}^2 + \overline{BD} + C\overline{D} - \overline{BC})(D^2 + AD + CD - AC) \\
&\quad - (D^2 + BD + CD - BC)(\overline{D}^2 + \overline{AD} + \overline{CD} - \overline{AC}) \\
&= \overline{A}BC\overline{D} + \overline{A}B\overline{C}D - A\overline{BC}D - A\overline{B}C\overline{D} - \overline{BC}D^2 - AC\overline{D}^2 + BC\overline{D}^2 \\
&\quad + \overline{AC}D^2 + A\overline{C} + \overline{B}C - \overline{A}C - B\overline{C} + 2A\overline{B} - 2\overline{A}B \\
&= (A - B)(\overline{C} - C\overline{D}^2) + (\overline{A - B})(\overline{C}D^2 - C) + (\overline{A}B - A\overline{B})(\overline{C}D + C\overline{D} - 2) \\
&= \frac{(A-B)(D^2 - C^2)}{CD^2} + \frac{(B-A)(D^2 - C^2)}{ABC} + \frac{(B^2 - A^2)(D - C)^2}{ABCD}.
\end{aligned}
$$

Thus, the equation of the Simson line is

$$
\begin{aligned}
&\frac{D}{2}\left[\frac{(D-C)(B-A)}{ABCD}\right]z - \frac{(C-D)(A-B)}{2D}\overline{z} \\
&\quad = \frac{1}{4}\left[\frac{(A-B)(D^2 - C^2)}{CD^2} + \frac{(B-A)(D^2 - C^2)}{ABC} + \frac{(B^2 - A^2)(D - C)^2}{ABCD}\right].
\end{aligned}
$$

Multiplying both sides by $\dfrac{2ABCD}{(D-C)(B-A)}$ gives the desired equation. □

Theorem 2.22. *Let $L, M, N \notin \{A, B, C\}$ be three distinct points on the circumcircle of $\triangle(ABC)$. The three Simson lines of L, M, N with respect to $\triangle(ABC)$ intersect if and only if $LMN = ABC$.*

Proof: We may assume the circumcircle of $\triangle(ABC)$ is $\mathbb{S}$. By Lemma 2.21, the equations of the Simson lines of L, M with respect to $\triangle(ABC)$ are

$$
\begin{aligned}
Lz - \sigma_3\overline{z} &= \frac{1}{2}(L^2 + \sigma_1 L - \sigma_2 - \frac{\sigma_3}{L}), \\
Mz - \sigma_3\overline{z} &= \frac{1}{2}(M^2 + \sigma_1 M - \sigma_2 - \frac{\sigma_3}{M})
\end{aligned}
$$

respectively, where $\sigma_1 = A+B+C$, $\sigma_2 = AB+AC+BC$, $\sigma_3 = ABC$. The intersection point t of these Simson lines thus satisfies

$$Lt - \frac{1}{2}(L^2 + \sigma_1 L - \frac{\sigma_3}{L}) = Mt - \frac{1}{2}(M^2 + \sigma_1 M - \frac{\sigma_3}{M}).$$

Therefore, $(L-M)t = \frac{1}{2}(L^2 - M^2 + (L-M)\sigma_1 + \frac{\sigma_3(L-M)}{LM})$ and $t = \frac{1}{2}(L+M+\sigma_1 + \frac{\sigma_3}{LM})$.

Similarly, the intersection point of the Simson lines of M and N wrt $\triangle(ABC)$ is $\frac{1}{2}(M+N+\sigma_1+\frac{\sigma_3}{MN})$. Thus, all three of the Simson lines intersect if and only if $L - N = \frac{\sigma_3(L-N)}{LMN}$ if and only if $LMN = \sigma_3$. □

Corollary 2.23. *Let A, B, C, L, M, N be distinct points on a circle. Then the Simson lines of the points L, M, N with respect to $\triangle(ABC)$ intersect if and only if the Simson lines of A, B, C with respect to $\triangle(LMN)$ intersect. In this case, all six Simson lines meet at $\dfrac{P+Q}{2}$ where P, Q are the orthocenters of $\triangle(ABC), \triangle(LMN)$ respectively.*

Proof: Assume the six points lie on $\mathbb{S}$. Then $P = A+B+C$ and $Q = L+M+N$. From the proof of Theorem 2.22, the Simson lines of L, M, N wrt $\triangle(ABC)$ (and of A, B, C wrt $\triangle(LMN)$ by symmetry) is $\frac{1}{2}[L+M+A+B+C+\frac{LMN}{LM}]$. □

Theorem 2.24. *Let W be a circle, $ABCD$ a quadrilateral with $A, B, C, D \in W$ and $P \in W - \{A, B, C, D\}$. Then the feet of the perpendiculars from P to the Simson lines of P with respect to $\triangle(ABC), \triangle(ABD), \triangle(ACD), \triangle(BCD)$ are collinear (on the* **Simson line** *of P wrt $ABCD$).*

Proof: We may assume $W = \mathbb{S}$. Then the Simson line L of P with respect to $\triangle(ABC)$ is $Pz - \sigma_3\overline{z} = \frac{1}{2}(P^2 + \sigma_1 P - \sigma_2 - \frac{\sigma_3}{P})$ where $\sigma_1 = A+B+C$, $\sigma_2 =$

$AB + AC + BC$, $\sigma_3 = ABC$. The equation of the line M with $P \in M$ and M perpendicular to L is $Pz + ABC\overline{z} = P^2 + \frac{ABC}{P}$. Thus, the foot Q of the perpendicular from P to L (i.e., $L \cap M$) is

$$\frac{1}{4P}[3P^2 + (A+B+C)P - (AB+AC+BC) + \frac{ABC}{P}].$$

Similarly, the foot R of the perpendicular from P to the Simson line of P wrt $\triangle(BCD)$ is

$$\frac{1}{4P}[3P^2 + (B+C+D)P - (BC+CD+BD) + \frac{BCD}{P}].$$

The line through Q and R has equation

$$P^2 z + \tau_4 \overline{z} = [3P^3 + \tau_1 P^2 - \tau_2 P + \tau_3 + \frac{3\tau_4}{P}]$$

where $\tau_1 = A + B + C + D$, $\tau_2 = AB + AC + AD + BC + BD + CD$, $\tau_3 = BCD + ACD + ABD + ABC$, $\tau_4 = ABCD$. But this equation is symmetric in A, B, C, D and therefore the other two feet also lie on this line. $\square$

Theorem 2.24 is part of an infinite sequence of theorems named for Robert Simson. The following result initiates yet another infinite sequence of theorems involving Simson lines. This sequence was discovered by M.B. Cantor. Its proof is similar to the above and is omitted here.

Theorem 2.25. *Let A, B, C, D, P, Q be cocyclic points in $\mathbb{P}^1_{\mathbb{E}}$ such that A, B, C, D are the vertices of a quadrilateral. Then the four intersections of the four pairs of Simson lines of the points P and Q with respect to $\triangle(BCD), \triangle(ACD), \triangle(ABD)$, $\triangle(ABC)$ are collinear (on the* **Cantor line** *of P and Q wrt $ABCD$).*

3. Hyperbolic Geometry.

Definition: Let $\mathbb{H} = \mathbb{E} - \mathbb{F}$ and $\mathbb{D} = \mathbb{P}^1_{\mathbb{E}} - \mathbb{S}$. We will call $\mathbb{H}$ the **plane model** and $\mathbb{D}$ the **disk model** of hyperbolic space.

Fix $\gamma \in \mathbb{I}$. Then $\phi(\mathbb{H}) = \mathbb{P}^1_{\mathbb{E}} - \mathbb{S}$ where $\phi(z) = \dfrac{1+\gamma z}{1-\gamma z}$. Also $\phi \in PGL_2(\ \mathbb{P}^1_{\mathbb{E}}\ )$ with inverse $\phi^{-1}(z) = \frac{z-1}{\gamma(z+1)}$. Recall that $PGL_2(\mathbb{F})$ acts transitively on $\mathbb{H}$ (Theorem 0.1) and thus $\phi PGL_2(\mathbb{F})\phi^{-1}$ acts transitively on $\mathbb{D}$ since ϕ is a bijection.

Remark: Since ϕ is an element of $PGL_2(\mathbb{E})$ and $PGL_2(\mathbb{E})_{\widehat{\mathbb{F}}} = PGL_2(\mathbb{F})$, $\phi PGL_2(\mathbb{F})\phi^{-1} = PGL_2(\mathbb{E})_{\phi(\widehat{\mathbb{F}})} = PGL_2(\mathbb{E})_{\mathbb{S}}$.

$$\text{Let } U := \left\{ \frac{-Bz - C}{\overline{C}z + \overline{B}} \mid B, C \in \mathbb{E},\ |B|^2 \neq |C|^2 \right\} \leq PGL_2(\mathbb{E}).$$

Lemma 3.1. $\phi PGL_2(\mathbb{F})\phi^{-1} = U$.

Proof: Given $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in PGL_2(\mathbb{F})$,

$$\begin{bmatrix} \gamma & 1 \\ -\gamma & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & -1 \\ \gamma & \gamma \end{bmatrix} = \begin{bmatrix} (a+d)\gamma + b\gamma^2 + c & (d-a)\gamma + b\gamma^2 - c \\ (d-a)\gamma - b\gamma^2 + c & (a+d)\gamma - b\gamma^2 - c \end{bmatrix} = \begin{bmatrix} -B & -C \\ \overline{C} & \overline{B} \end{bmatrix}.$$

where $B = -(a+d)\gamma - (b\gamma^2 + c),\ C = (a-d)\gamma - b\gamma^2 + c$.

Now
$|B|^2 = (\ -(a+d)\gamma - (b\gamma^2 + c\ ))(\ (a+d)\gamma - (b\gamma^2 + c)\ ) = -2\gamma^2(ad - bc)$,

$|C|^2 = (\ (a-d)\gamma - b\gamma^2 + c\ )(\ -(a-d)\gamma - b\gamma^2 + c\ ) = 2\gamma^2(ad - bc)$.
Since $ad - bc \neq 0$, $|B|^2 \neq |C|^2$ and $\phi PGL_2(\mathbb{F})\phi^{-1} \subseteq U$.

Let $g(z) = \dfrac{-(Bz + C)}{\overline{C}z + \overline{B}} \in U$. By the above remark, it suffices to check that $g(\mathbb{S}) = \mathbb{S}$. Given $x \in \mathbb{S}$,

$$g(x)\overline{g(x)} = \left[\frac{-(Bx + C)}{\overline{C}x + \overline{B}}\right]\left[\frac{-(\overline{Bx + C})}{C\overline{x} + B}\right] = \frac{B\overline{B}x\overline{x} + \overline{B}C\overline{x} + B\overline{C}x + C\overline{C}}{C\overline{C}x\overline{x} + \overline{B}C\overline{x} + B\overline{C}x + B\overline{B}} = 1. \quad \square$$

Lemma 3.2. *The ratio* $\dfrac{-|z-w|^2}{(z-\overline{z})(w-\overline{w})}$ *is preserved by* $PGL_2(\mathbb{F})$ *where* $z,w \in \mathbb{H}$.

Proof: Let $g(z) = \frac{az+b}{cz+d} \in PGL_2(\mathbb{F})$. Then

$$g(z) - g(w) = \frac{(az+b)(cw+d)-(aw+b)(cz+d)}{(cz+d)(cw+d)} = (ad-bc)(z-w).$$

Since $g \in PGL_2(\mathbb{F})$ and thus commutes with $\overline{z}$, $\overline{g(z)} = g(\overline{z})$. Thus,

$$\frac{-[\,(g(z)-g(w))(\overline{g(z)-g(w)})\,]}{(g(z)-\overline{g(z)})(g(w)-\overline{g(w)})} = \frac{-(ad-bc)^2(z-w)(\overline{z-w})}{(ad-bc)^2(z-\overline{z})(w-\overline{w})} = \frac{-|z-w|^2}{(z-\overline{z})(w-\overline{w})}. \qquad \square$$

Definition: The **hyperbolic distance** between $z,w \in \mathbb{H}$ is

$$\triangle'(z,w) = \frac{-|z-w|^2}{(z-\overline{z})(w-\overline{w})}.$$

The hyperbolic distance between $x,y \in \mathbb{D}$ is $\triangle(x,y) := \triangle'(\phi^{-1}(x),\phi^{-1}(y))$.

Since $\triangle'$ is invariant under $PGL_2(\mathbb{F})$, $\triangle$ is invariant under $\phi PGL_2(\mathbb{F})\phi^{-1}$.

Lemma 3.3. $\triangle(x,y) = \dfrac{|x-y|^2}{(1-|x|^2)(1-|y|^2)}$ *if* $x,y \in \mathbb{D}-\{\infty\}$ *and* $\triangle(x,y) = \dfrac{1}{|y|^2-1}$ *if* $x=\infty$.

Proof: If $x,y \in \mathbb{D}-\{\infty\}$, then

$$\begin{aligned}
\phi^{-1}(x)-\phi^{-1}(y) &= \frac{x-1}{\gamma(x+1)} - \frac{y-l}{\gamma(y+1)} = \frac{2(x-y)}{\gamma(x+1)(y+1)}, \\
\phi^{-1}(x)-\overline{\phi^{-1}(x)} &= \frac{x-1}{\gamma(x+1)} + \frac{\overline{x}-1}{\gamma(\overline{x}+1)} = \frac{-2(1-|x|^2)}{\gamma|x+1|^2}.
\end{aligned}$$

Thus,

$$\begin{aligned}
\frac{-|\phi^{-1}(x)-\phi^{-1}(y)|^2}{(\phi(x)-\overline{\phi(x)})(\phi(y)-\overline{\phi(y)})} &= \frac{4|x-y|^2}{\gamma^2|x+1|^2|y+1|^2} \div \frac{4(1-|x|^2)(1-|y|^2)}{\gamma^2|x+1|^2|y+1|^2} \\
&= \frac{|x-y|^2}{(1-|x|^2)(1-|y|^2)}.
\end{aligned}$$

If $x = \infty$, then $\phi^{-1}(x) = \frac{1}{\gamma}$, $\phi^{-1}(x) - \phi^{-1}(y) = \frac{2}{\gamma(y+1)}$ and $\phi^{-1}(x) - \overline{\phi^{-1}(x)} = \frac{2}{\gamma}$. Thus,

$$\triangle(x,y) = \left(\frac{4}{\gamma^2|y+1|^2}\right) \div \left(\frac{-4(1-|y|^2)}{\gamma^2|y+1|^2}\right) = \frac{-1}{1-|y|^2} = \frac{1}{|y|^2-1}. \quad \square$$

Note that $\triangle(z,w) \in \mathbb{F}$ for all $z, w \in \mathbb{H}$ since $z - \overline{z},\ w - \overline{w} \in \mathbb{I} - \{0\}$. Also $\triangle(z,w) = \triangle(w,z)$ and $\triangle(z,w) = 0$ if and only if $z = w$.

Definition: Points $A, B \in \mathbb{D}$ are **conjugate in** $\mathbb{D}$ if and only if $\phi^{-1}(A), \phi^{-1}(B)$ are conjugate in $\mathbb{H}$.

Lemma 3.4.

i) $\triangle'(z,w) = -1$ *if and only if* $w = \overline{z}$.

ii) $\triangle(A,B) = -1$ *if and only if* A, B *are conjugate in* $\mathbb{D}$ *if and only if* $B = \dfrac{1}{\overline{A}}$.

Proof: i)

$$\begin{aligned}\triangle'(z,w) = -1 &\iff (z-w)(\overline{z-w}) = (z-\overline{z})(w-\overline{w}) \\ &\iff z\overline{z} - zw - \overline{wz} + w\overline{w} = 0 \\ &\iff (z-\overline{w})(\overline{z}-w) = 0 \iff w = \overline{z}.\end{aligned}$$

ii) Assume $A, B \in \mathbb{D} - \{0, \infty\}$. Then

$$\begin{aligned}\triangle(A,B) = -1 &\iff \triangle'(\phi^{-1}(A), \phi^{-1}(B)) = -1 \\ &\iff \frac{\overline{B}-1}{-\gamma(\overline{B}+1)} = \overline{\phi^{-1}(B)} = \phi^{-1}(A) = \frac{A-1}{\gamma(A+1)} \\ &\iff (\overline{B}-1)(A+1) = -(A-1)(\overline{B}+1) \\ &\iff A\overline{B} - 1 = -A\overline{B} + 1 \iff A\overline{B} - 1 = 0 \iff \overline{B} = \frac{1}{A}.\end{aligned}$$

If $A = 0$, then

$$\triangle(0,B) = -1 \iff \triangle'(\frac{-1}{\gamma}, \phi^{-1}(B)) = -1 \iff \phi^{-1}(B) = \frac{1}{\gamma} \iff B = \infty. \quad \square$$

Definition: Let $\lambda \in \mathbb{F}^{\times} - \{-1\}$, $a \in \mathbb{H}$, $b \in \mathbb{D}$. The **hyperbolic circle** with sqradius λ and center a in $\mathbb{H}$ (respectively center b in $\mathbb{D}$) is $\{\, z \in \mathbb{H} \mid \triangle'(z,a) = \lambda \,\}$ (respectively $\{z \in \mathbb{D} \mid \triangle(z,b) = \lambda \,\}$).

Proposition 3.5. *Let* $\lambda \in \mathbb{F}^{\times} - \{-1\}$, $b \in \mathbb{H}$.

i) $\{\, z \in \mathbb{D} \mid \triangle(z,0) = \lambda \,\} = \left(\frac{\lambda}{\lambda+1}\right)\mathbb{S}$

ii) $\{\, z \in \mathbb{H} \mid \triangle'(z,b) = \lambda \,\} = c\mathbb{S} + d$ *for some* $c \in \mathbb{E}^{\times}$, $d \in \mathbb{E}$.

Proof: i) $\triangle(z,0) = \lambda \iff \dfrac{z\overline{z}}{1 - z\overline{z}} = \lambda \iff \lambda = (\lambda+1)z\overline{z} \iff z\overline{z} = \dfrac{\lambda}{\lambda+1}$.

ii) Let $C = \{\, z \in \mathbb{H} \mid \triangle'(z,b) = \lambda \,\}$. Then $\phi(C) = \{\, w \in \mathbb{D} \mid \triangle(w, \phi(b)) = \lambda \,\}$. Since $\phi PGL_2(\mathbb{F})\phi^{-1}$ acts transitively on $\mathbb{D}$ and preserves $\triangle$, we may assume that $\phi(C) = \{\, w \in \mathbb{D} \mid \triangle(w,0) = \lambda \,\} = \left(\frac{\lambda}{\lambda+1}\right)\mathbb{S}$. Thus, $C = \phi^{-1}\left(\left(\frac{\lambda}{\lambda+1}\right)\mathbb{S} \right)$ is a mirror since $\phi^{-1} \in PGL_2(\mathbb{E})$. But $C \subseteq \mathbb{H}$ and $\infty \notin \mathbb{H}$, so C must be a Euclidean circle. $\square$

Remark:

i) Let W be a hyperbolic circle in $\mathbb{D}$ centered at p and $Q \in W$. Since $U \subseteq PGL_2(\mathbb{E})$ and acts transitively on $\mathbb{D}$, Proposition 3.5(i) implies that W is a mirror. Note that it is possible for a hyperbolic circle in $\mathbb{D}$ to be an extended line. (If $g \in U$ and $g(Q) = \infty$, then $g(W)$ is a hyperbolic circle centered at $g(P)$ and containing ∞.

ii) It is possible for two hyperbolic circles with different centers to be equal.

For example, if $\mathbb{F} = \mathbb{F}_3$, then

$$\{ z \in \mathbb{H} \mid \Delta'(z,i) = 1 \} = \{1 \pm i, -1 \pm i\} = \{z \in \mathbb{H} \mid \Delta'(z,-i) = 1 \}.$$

Lemma 3.6. *Let A, B, C be distinct points of $\mathbb{D}$, $C \neq \infty$.*

i) $\Delta(0,A) = \Delta(0,B)$ *if and only if* $A\overline{A} = B\overline{B}$.

ii) *If* $\Delta(0,A) = \Delta(0,B)$, *then* $\Delta(C,A) = \Delta(C,B)$ *if and only if* $0C \perp AB$.

Proof: i) $\dfrac{A\overline{A}}{1-A\overline{A}} = \dfrac{B\overline{B}}{1-B\overline{B}}$ if and only if $A\overline{A} = B\overline{B}$.

ii)

$$\begin{aligned}
\Delta(C,A) = \Delta(C,B) &\iff \frac{(C-A)(\overline{C-A})}{1-A\overline{A}} = \frac{(C-B)(\overline{C-B})}{1-B\overline{B}} \\
&\iff -A\overline{C} - \overline{A}C = -B\overline{C} - \overline{B}C \\
&\iff -\overline{C}(A-B) = C(\overline{A-B}) \\
&\iff den(AB, 0C) = \frac{C(\overline{A-B})}{\overline{C}(A-B)} = -1. \quad \square
\end{aligned}$$

Lemma 3.7. $\Delta'(z,A) + \Delta'(z,\overline{A}) = -1$ *for all* $A \in \mathbb{H}$.

Proof: Let $R = (z-\overline{z})(A-\overline{A})$ and $X = z\overline{z} + A\overline{A}$. Then

$$\begin{aligned}
\Delta'(z,A) &= \frac{-(z-A)(\overline{z-A})}{R} = \frac{A\overline{z} + \overline{A}z - X}{R}, \\
\Delta'(z,\overline{A}) &= \frac{(z-\overline{A})(\overline{z}-A)}{R} = \frac{X - \overline{Az} - Az}{R}.
\end{aligned}$$

Therefore,

$$\Delta'(z,\overline{A}) + \Delta'(z,A) = \frac{A\overline{z} + \overline{A}z - \overline{Az} - Az}{R} = \frac{(A-\overline{A})(\overline{z}-z)}{R} = -1. \quad \square$$

Theorem 3.8. *Let* $C = \{ z \in \mathbb{H} \mid \Delta'(z, A) = \lambda \}$, $W = \{ z \in \mathbb{H} \mid \Delta'(z, B) = \mu \}$ *where* $A \neq B \in \mathbb{H}$ *and* $\lambda, \mu \in \mathbb{F}^\times - \{-1\}$. *Then* $C = W$ *if and only if* $B = \overline{A}$ *and* $\mu = -(\lambda + 1)$.

Proof: If $B = \overline{A}$, then $C = W$ if and only if $\mu = -(\lambda + 1)$ by Lemma 3.7. Suppose $C = W$ and $B \neq \overline{A}$. Working in the disk model, WMA $A = 0$. Since $C = W$, pick $P \neq Q \neq R \in C \cap W$. Since $B \neq \infty$, $\Delta(0, P) = \lambda = \Delta(0, Q)$ and $\Delta(B, P) = \mu = \Delta(B, Q)$, we have $OB \perp PQ$ by Lemma 3.6(ii). Similarly, $0B \perp PR$. But then $PQ = PR$ and P, Q, R are collinear. This is a contradiction since P, Q, R determine the Euclidean circle C. $\square$

Remark: If $A, B \in \mathbb{H}$ with $A \notin \{B, \overline{B}\}$ and $\lambda \in \mathbb{F}^\times - \{-1\}$, then $| \{z \in \mathbb{H} \mid \Delta'(z, A) = \lambda = \Delta'(z, B) \} | \leq 2$. ($C = \{ z \in \mathbb{H} | \Delta'(z, A) = \lambda \}$ and $D = \{ z \in \mathbb{H} | \Delta'(z, B) = \lambda \}$ are distinct Euclidean circles and thus $| C \cap D | \leq 2$.)

Lemma 3.9. *Let* $a \neq b \in \mathbb{I} - \{0\}$, $\lambda, \mu \in \mathbb{F}^\times - \{-1\}$.

Let $C = \{ z \in \mathbb{H} \mid \Delta'(z, a) = \lambda \}$, $W = \{ z \in \mathbb{H} \mid \Delta'(z, b) = \mu \}$.

i) *For* x, $y \in \mathbb{H}$, $\Delta'(x, y) = \Delta'(-\overline{x}, y)$ *if and only if* $x \in \mathbb{I} - \{0\}$ *or* $y \in \mathbb{I} - \{0\}$.

ii) $P \in C$ *if and only if* $-\overline{P} \in C$.

iii) *If* $t \in C \cap W$ *and* $C \neq W$, *then* $C \cap W = \{ t, -\overline{t} \}$.

Proof: i)

$$\begin{aligned}\triangle'(x,y) &= \frac{-|x-y|^2}{(x-\overline{x})(y-\overline{y})} = \frac{-|-\overline{x}-y|^2}{(x-\overline{x})(y-\overline{y})} = \triangle'(-\overline{x},y)\\ &\iff (-\overline{x}-y)(\overline{-\overline{x}-y}) = x\overline{x}+xy+\overline{x}\overline{y}+y\overline{y}\\ &\qquad\qquad = x\overline{x}-\overline{x}y-x\overline{y}+y\overline{y} = (x-y)(\overline{x-y})\\ &\iff (x+\overline{x})(y+\overline{y})=0 \iff x\in\mathbb{I}-\{0\} \text{ or } y\in\mathbb{I}-\{0\}.\end{aligned}$$

ii) Since $a\in\mathbb{I}-\{0\}$, $\triangle'(P,a)=\triangle'(-\overline{P},a)$ by i).

iii) Since $a,b\in\mathbb{I}-\{0\}$, $-\overline{t}\in C\cap W$. So $\{\,t,-\overline{t}\,\}\subseteq C\cap W$. Note that $\mathbb{I}$ is orthogonal to both C and W since C and W are invariant under $-\overline{z}$. Consequently, the Euclidean centers $\widetilde{a},\widetilde{b}$ of C,W respectively both lie on $\mathbb{I}$. If $r\in C\cap W$, $r\notin\{\,t,-\overline{t}\,\}$, then $r,t\in\mathbb{I}$ since $|\,C\cap W\,|\leq 2$. This is a contradiction to Lemma 1.32(ii). Thus, $C\cap W=\{\,t,-\overline{t}\,\}$. □

Lemma 3.10.

i) $PGL_2(\mathbb{F})_{\frac{-1}{\gamma}} = \{\ \begin{bmatrix} a & b\\ b\gamma^2 & a\end{bmatrix}\ |\ a,b\in\mathbb{F},\ a\neq 0 \text{ or } b\neq 0\ \}$.

ii) $\left(\phi PGL_2(\mathbb{F})\phi^{-1}\right)_0 = \mathbb{S}z$.

iii) *$\mathbb{S}z$ acts sharply transitively on any hyperbolic circle in $\mathbb{D}$ centered at* 0.

Proof: i) Let $g(z)=\dfrac{az+b}{cz+d}\in PGL_2(\mathbb{F})$. If $z\in\mathbb{H}$, then $g(z)=z$ iff $cz^2-(a-d)z-b=0$ iff $p(z)=z^2-\dfrac{(a-d)}{c}z-\dfrac{b}{c}=0$. Thus, $g\left(\frac{-1}{\gamma}\right)=\frac{-1}{\gamma}$ iff $\frac{-1}{\gamma}$ is a root of $p(z)$ iff $\left(\overline{\frac{-1}{\gamma}}\right)=\frac{1}{\gamma}$ is a root of $p(z)$. But the unique monic quadratic having roots $\{\ \frac{-1}{\gamma},\frac{1}{\gamma}\ \}$ is $z^2-\frac{1}{\gamma^2}$. So $g\left(\frac{-1}{\gamma}\right)=\frac{-1}{\gamma}$ iff $p(z)=z^2-\frac{1}{\gamma^2}$ iff $a=d$ and $c=b\gamma^2$. Also

$$\det(g)=\begin{vmatrix} a & b\\ b\gamma^2 & a\end{vmatrix} = a^2-b^2\gamma^2\neq 0 \implies a\neq 0 \text{ or } b\neq 0.$$

Conversely, assume without loss of generality that $b \neq 0$. If $a^2 = b^2\gamma^2$, then $\gamma^2 = \frac{a^2}{b^2} \in \mathbb{F}^\times$ and $\gamma = \pm\frac{a}{b} \in \mathbb{F} \cap (\mathbb{I} - \{0\}) = \emptyset$. Thus, $a^2 \neq b^2\gamma^2$.

ii) Let $g \in PGL_2(\mathbb{F})$. Since $\phi^{-1}(0) \neq \frac{-1}{\gamma}$, $\phi g \phi^{-1}(0) = 0$ iff $g\left(\frac{-1}{\gamma}\right) = \frac{-1}{\gamma}$. Thus,

$$\begin{aligned}
\left(\phi PGL_2(\mathbb{F})\phi^{-1}\right)_0 &= \phi(PGL_2(\mathbb{F})_{\frac{-1}{\gamma}})\phi^{-1} \\
&= \left\{ \begin{bmatrix} \gamma & 1 \\ -\gamma & 1 \end{bmatrix} \begin{bmatrix} a & b \\ a\gamma^2 & a \end{bmatrix} \begin{bmatrix} 1 & -1 \\ \gamma & \gamma \end{bmatrix} \mid a, b \in \mathbb{F},\ a \neq 0 \text{ or } b \neq 0 \right\} \\
&= \left\{ \begin{bmatrix} 2(a\gamma + b\gamma^2) & 0 \\ 0 & 2(a\gamma - b\gamma^2) \end{bmatrix} \mid a, b \in \mathbb{F},\ a \neq 0 \text{ or } b \neq 0 \right\} \\
&= \left\{ \begin{bmatrix} a + b\gamma & 0 \\ 0 & a - b\gamma \end{bmatrix} \mid a, b \in \mathbb{F}, a \neq 0 \text{ or } b \neq 0 \right\}.
\end{aligned}$$

Since $\rho(a + b\gamma)z = \frac{a+b\gamma}{\overline{a}+\overline{b}\overline{\gamma}}z \in \mathbb{S}z$ and ρ maps onto $\mathbb{S}$, $\left(\phi PGL_2(\mathbb{F})\phi^{-1}\right)_0 = \mathbb{S}z$.

iii) Let $C = \{\ w \in \mathbb{D} \mid \triangle(w, 0) = \lambda\ \} = \mu\mathbb{S}$ where $\mu = \frac{\lambda}{\lambda+1}$. Since $\mathbb{S}z = B_{\mu\mathbb{S}}$ is the group of Euclidean rotations with respect to $\mu\mathbb{S}$, the result follows from Lemma 1.27. $\square$

Proposition 3.11. *If $\triangle'(z, w) = \lambda = \triangle'(x, y)$, then there exists $g \in PGL_2(\mathbb{F})$ such that $g(x) = z$, $g(y) = w$. If $\lambda \in \mathbb{F}^\times - \{-1\}$, then g is unique.*

Proof: Now $z = w$, $x = y$ if $\lambda = 0$ and $w = \overline{z}$, $y = \overline{x}$ if $\lambda = -1$. In either case, there exists a $g \in PGL_2(\mathbb{F})$ such that $g(x) = z$ by transitivity. If $\lambda = -1$, then $g(y) = g(\overline{x}) = \overline{z} = w$ since g commutes with $\overline{z}$. Assume $\lambda \in F^\times - \{-1\}$. It suffices to show there exists $h \in \phi PGL_2(\mathbb{F})\phi^{-1}$ such that $h(c) = a, h(d) = b$ when $\triangle(a, b) = \lambda = \triangle(c, d)$. Since $\phi PGL_2(\mathbb{F})\phi^{-1}$ acts transitively on $\mathbb{D}$, we may assume $a = c = 0$. Then b, d are in $C = \{\ k \in \mathbb{D} \mid \triangle(k, 0) = \lambda\ \}$. By Lemma 3.6(iii), there is an element $h \in \mathbb{S}z$ such that $h(d) = b$ (and $h(0) = 0$). $\square$

Lemma 3.12. *Let $a, b \in \mathbb{H}$ with $a \notin \{ b, \overline{b} \}$. The unique $g \in PGL_2(\mathbb{F})$ with $g(a) = b$ and $g(b) = a$ has order two.*

Proof: Since $\triangle'(a,b) = \triangle'(b,a) \in \mathbb{F}^{\times} - \{-1\}$, there is a unique $g \in PGL_2(\mathbb{F})$ with $g(a) = b,\ g(b) = a$ by Proposition 3.11. Now $g^2 \in PGL_2(\mathbb{F})$ fixes the three distinct points $a, b, \overline{a}$. Thus, $g^2 = 1$. $\square$

Definition: A bijection $\tau : \mathbb{H} \mapsto \mathbb{H}$ preserving $\triangle'$ is said to be an **isometry** of $(\mathbb{H}, \triangle')$.

The set of all isometries of $(\mathbb{H}, \triangle')$ forms a group under composition denoted Isom($\mathbb{H}$,$\triangle'$).

The group Isom($\mathbb{D}$,$\triangle$) is defined analogously.

Theorem 3.13. *Assume $\mathbb{F} \neq \mathbb{F}_3$. Let $a,\ b \in \mathbb{I} - \{0\}$ such that $a \notin \{ b, \overline{b} \}$ and $c \in \mathbb{H} - \mathbb{I}$. If $g \in$ Isom($\mathbb{H}, \triangle'$) fixing both a and b, then $g = 1$ if g also fixes c and $g = -\overline{z}$ otherwise.*

Proof: Now $\triangle'(a, g(\overline{a})) = \triangle'(a, \overline{a}) = -1 \implies g(\overline{a}) = \overline{a}$. Similarly, $g(\overline{b}) = \overline{b}$. Let $t \in \mathbb{I} - \{ 0, a, \overline{a}, b, \overline{b} \}$. Then $\triangle'(a,t) = \lambda,\ \triangle'(b,t) = \mu \in \mathbb{F}^{\times} - \{-1\}$. Note that $\{ t, g(t) \} \subseteq C \cap W$ where $C = \{ z \in \mathbb{H} \mid \triangle'(z,a) = \lambda \}$, $W = \{ z \in \mathbb{H} \mid \triangle'(z,b) = \mu \}$. Since $C \neq W$ and $t \in \mathbb{I} - \{0\}$, $C \cap W = \{t\}$ by Lemma 3.9(iii). Thus, $g(t) = t$ for every $t \in \mathbb{I} - \{0\}$.

Arguing as above, we also have that $g(x) \in \{ x, -\overline{x} \}$ for all $x \in \mathbb{H} - \mathbb{I}$. Let $h = g$ if $g(C) = C$ and $h = (-\overline{z}) \circ g$ if $g(C) = -\overline{C}$. Then h fixes $\mathbb{I} - \{0\}$ pointwise and $h(C) = C$. Let $c \neq r \in \mathbb{H} - \mathbb{I}$. Now $\triangle'(h(r), c) = \triangle'(r, c) \neq \triangle'(-\overline{r}, c)$ by Lemma 3.9(i). Thus, $h(r) = r$ and $h = 1$. Consequently, $g = 1$ if $g(C) = C$ and

$g = -\overline{z}$ otherwise. $\square$

Corollary 3.14. *Assume* $\mathbb{F} \neq \mathbb{F}_3$, *Then Isom(* $\mathbb{H}, \triangle'$) $= < PGL_2(\mathbb{F}), -\overline{z} >$ *and Isom(* $\mathbb{D}, \triangle$) $= < \phi PGL_2(\mathbb{F})\phi^{-1}, \overline{z} >$.

Proof: Both $PGL_2(\mathbb{F})$ and $-\overline{z}$ clearly preserve $\mathbb{F}$ and thus $\mathbb{H}$. Since $-\overline{z}$ also preserves $\triangle'$, $< PGL_2(\mathbb{F}), -\overline{z} > \subseteq$ Isom($\mathbb{H}, \triangle'$) by Lemma 3.2. Let $g \in$ Isom($\mathbb{H}, \triangle'$). Let a, b be in $\mathbb{I} - \{0\}$ such that $a \notin \{ b, \overline{b}\}$. Since $\triangle'(g(a), g(b)) = \triangle'(a, b)$, there exists $k \in PGL_2(\mathbb{F})$ such that $k(g(a)) = a$ and $k(g(b)) = b$. Thus, $k \circ g = 1$ or $k \circ g = -\overline{z}$ by Theorem 3.13. Consequently, $g = k^{-1}$ or $g = k^{-1} \circ (-\overline{z})$ and $g \in < PGL_2(\mathbb{F}), -\overline{z} >$.

It is immediate that Isom($\mathbb{D}, \triangle$) $= < \phi PGL_2(\mathbb{F})\phi^{-1}, \overline{z} >$ since $\phi \circ (-\overline{z}) \circ \phi^{-1} = \overline{z}$. $\square$

Remarks:

i) Since $-1 \in PGL_2(\mathbb{F})$, $< PGL_2(\mathbb{F}), -\overline{z} > = < PGL_2(\mathbb{F}), \overline{z} >$.

ii) We will use the two models of hyperbolic space interchangeably from now on.

Definition: A reflection is a **hyperbolic reflection of** $\mathbb{H}$ if and only if its mirror is orthogonal to $\widehat{\mathbb{F}}$.

Equivalently, a reflection r_L is a hyperbolic reflection of $\mathbb{H}$ if and only if L is (an extended) vertical line or a Euclidean circle centered on $\mathbb{F}$.

By Remark(ii) above and Proposition 2.15(iii), hyperbolic reflections are isometries of ($\mathbb{H}, \triangle'$).

Lemma 3.15. *If $g, h \in$ Isom($\mathbb{H}$,$\triangle'$) and g, $h \notin PGL_2(\mathbb{F})$, then $gh \in PGL_2(\mathbb{F})$.*

Proof: Now $PGL_2(\mathbb{F})$ has index two in Isom($\mathbb{H}$,$\triangle'$), so $g^{-1}, h \notin PGL_2(\mathbb{F})$ implies $g^{-1}PGL_2(\mathbb{F}) = hPGL_2(\mathbb{F})$. Consequently, $gh \in PGL_2(\mathbb{F})$. □

In particular, the product of $r_C \circ r_W$ of two hyperbolic reflections is in $PGL_2(\mathbb{F})$.

Given two distinct points $\alpha, \beta \in \mathbb{E}$, there is always a Euclidean reflection r_L such that $r_L(\alpha) = \beta$; namely, let L be the perpendicular bisector of $\alpha\beta$. We now determine the conditions for the existence of a hyperbolic reflection taking α to β.

Proposition 3.16. *Let $\alpha \neq \beta \in \mathbb{H}$.*

i) *There is a vertical line L such that $r_L(\alpha) = \beta$ if and only if $\alpha\beta \parallel \mathbb{F}$.*

ii) *Assume $t \in \alpha\beta \cap \mathbb{F}$ and $\alpha \neq \overline{\beta}$. There is a Euclidean circle C centered on $\mathbb{F}$ such that $r_C(\alpha) = \beta$ if and only if $\dfrac{\beta - t}{\alpha - t} \in$ Im(N).*

Proof: i) If $\alpha\beta \parallel \mathbb{F}$, then the perpendicular bisector L of $\alpha\beta$ is perpendicular to $\mathbb{F}$ and thus L is a vertical line with $r_L(\alpha) = \beta$. Conversely, if $r_M(\alpha) = \beta$ where M is a vertical line, then $r_M(\alpha\beta) = \alpha\beta$ and $M \perp \alpha\beta$. Thus, $\alpha\beta \parallel \mathbb{F}$.

ii) Since den($\alpha\beta$,$\alpha\beta$) $= 1$, $\lambda = \dfrac{\beta - t}{\alpha - t} \in \mathbb{F}^{\times}$. Translating if necessary, we may assume $t = 0$. Let $C = a\mathbb{S} + b$ with $b \in \mathbb{F}$. Then $r_C(z) = \dfrac{a\overline{a}}{\overline{z} - b} + b$. Now

$$r_C(\alpha) = \beta \quad \text{and} \quad r_C(\beta) = \alpha$$

$$\iff \frac{a\overline{a}}{\overline{\alpha}-b}+b=\lambda\alpha \text{ and } \frac{a\overline{a}}{\lambda\overline{\alpha}-b}+b=\alpha$$

$$\iff a\overline{a}+b\overline{\alpha}-b^2=\lambda\alpha\overline{\alpha}-\lambda\alpha b \text{ and } a\overline{a}+\lambda b\overline{\alpha}-b^2=\lambda\alpha\overline{\alpha}-\alpha b$$

$$\iff b^2-(\overline{\alpha}+\lambda\alpha)b+(\lambda\alpha\overline{\alpha}-a\overline{a})=0=b^2-(\lambda\overline{\alpha}+\alpha)b+(\lambda\alpha\overline{\alpha}-a\overline{a}).$$

If $b\neq 0$, then $\overline{\alpha}+\lambda\alpha=\lambda\overline{\alpha}+\alpha$ and $(\lambda-1)(\alpha-\overline{\alpha})=0$. Since $\alpha\in\mathbb{H}-\{\beta\}$, $b=0$. Thus, $r_C(z)=\dfrac{a\overline{a}}{\overline{z}}$ with $r_C(\alpha)=\beta$ iff $a\overline{a}=\lambda\alpha\overline{\alpha}$ iff $r_C(z)=\dfrac{\lambda\alpha\overline{\alpha}}{\overline{z}}$. But $C=(\lambda\alpha\overline{\alpha})\mathbb{S}+b$ is a circle if and only if $\lambda\alpha\overline{\alpha}\in \mathrm{Im}(N)$ if and only if $\lambda\in\mathrm{Im}(N)$. □

In particular, if N is surjective, then there is always a hyperbolic reflection taking α to β for $\alpha\neq\beta\in\mathbb{H}$.

Theorem 3.17. *If N is surjective, then every element of $PGL_2(\mathbb{F})$ is a product of two hyperbolic reflections.*

Proof: WMA $1\neq g\in PGL_2(\mathbb{F})$. Choose $\alpha\in\mathbb{H}$ with $g(\alpha)\neq\{\alpha,\overline{\alpha}\}$. By Proposition 3.16, there exists a hyperbolic reflection such that $\rho(\alpha)=g(\alpha)$. Thus, $\rho\circ g(\alpha)=\alpha$ and $\rho\circ g(\overline{\alpha})=\overline{\alpha}$. Let $\tau=\phi\circ\rho\circ g\circ\phi^{-1}$. Now τ fixes $\phi(\alpha)$ and $\phi(\overline{\alpha})$. By transitivity, we may assume $\phi(\alpha)=0$ so that τ fixes 0 and ∞.

Let $x\in\mathbb{D}-\{0,\infty\}$. Then $x,\tau(x)\in C=\{\ z\in\mathbb{D}\mid\triangle(z,0)=x\ \}$, a Euclidean circle also centered at 0. By Lemma 1.32(i), $L=0\left(\dfrac{x+\tau(x)}{2}\right)$ is the perpendicular bisector of $x\tau(x)$ and $r_L(\tau(x))=x$. Since $r_L\circ\tau$ fixes $0,\infty$, and x,

$$\phi^{-1}\circ(r_L\circ\tau)\circ\phi=(\phi^{-1}\circ r_L\circ\phi)(\rho\circ g)=r_M\circ\rho\circ g\in PGL_2(\mathbb{F})$$

fixes $\alpha,\overline{\alpha}$ and $\phi^{-1}(x)$ where $M=\alpha\phi^{-1}(x)$. Consequently, $r_M\circ\rho\circ g=1$ and $g=\rho\circ r_M$. Since $0,\infty\in L$, M contains two conjugate points and must therefore be either a vertical line or a circle centered on $\mathbb{F}$. Hence, r_M is a hyperbolic reflection. □

Definition: A **hyperbolic mirror** of the plane model is a mirror of a hyperbolic reflection of $\mathbb{H}$ intersected with $\mathbb{H}$. A hyperbolic mirror of the disk model is $\phi(G)$ where G is a hyperbolic mirror of $\mathbb{H}$.

For convenience, we will refer to a mirror C as being hyperbolic when we really mean $\mathbb{H} \cap C$ is hyperbolic. In this notation, the hyperbolic mirrors of $\mathbb{H}$ are all mirrors of $\mathbb{P}^1_{\mathbb{E}}$ which are orthogonal to $\widehat{\mathbb{F}}$. Therefore, the hyperbolic mirrors of $\mathbb{D}$ are all mirrors of $\mathbb{P}^1_{\mathbb{E}}$ which are orthogonal to $\mathbb{S}$.

Lemma 3.18. *Let C be a mirror in $\mathbb{P}^1_{\mathbb{E}}$.*

i) *If C is an extended line, then C is a hyperbolic mirror of $\mathbb{D}$ if and only if $0 \in C$.*

ii) *If $C = a\mathbb{S}+b$, then C is a hyperbolic mirror of $\mathbb{D}$ if and only if $a\bar{a} = b\bar{b}-1$.*

Proof: i) $C \Psi \mathbb{S}$ if and only if the center 0 of $\mathbb{S}$ lies on C.

ii) By Proposition 2.16, $C \Psi \mathbb{S}$ if and only if $a\bar{a} + 1 = b\bar{b}$. □

Remarks:

i) If $0 \in a\mathbb{S}+b$, then $a\bar{a} = b\bar{b}$. Thus, it follows from Lemma 3.18(ii) that the only hyperbolic mirrors of $\mathbb{D}$ passing through 0 are lines. It also follows that the only hyperbolic mirror of $\mathbb{D}$ of the form $a\mathbb{S}$ is T.

ii) Assume $\mathbb{F} \neq \mathbb{F}_3$ and let G and H be distinct hyperbolic mirrors of $\mathbb{H}$. Since neither G nor H contains more than two points of $\mathbb{F}$, $|\mathbb{F} \cap (G \cup H)| \leq$

4. Thus, there is a point $t \in \mathbb{F} - (G \cup H)$. By a change of coordinates, we may assume that t is infinity. Then G and H are both Euclidean circles centered on $\mathbb{F}$. Since $PGL_2(\mathbb{F})$ acts doubly transitively on $\widehat{\mathbb{F}}$, we may further assume G is centered at 0 and H is centered at 1.

The following is a more constructive proof of Theorem 3.17 but requires the additional hypothesis that $\mathbb{F} \subseteq \mathbb{E}_+$.

Theorem 3.19. *Assume $\mathbb{F} \neq \mathbb{F}_3$ and $\mathbb{F} \subseteq \mathbb{E}_+$. Then every element of $PSL_2(\mathbb{F})$ is a product of two hyperbolic reflections. If, in addition, N is surjective, then every element of $PGL_2(\mathbb{F})$ is also a product of two hyperbolic reflections. Moreover, if $1 \neq g = r_C r_D$ is in $PGL_2(\mathbb{F})$ for hyperbolic mirrors C and D, then*

i) *g is parabolic if and only if C, D are tangent (at a point in $\widehat{\mathbb{F}}$).*

ii) *g is hyperbolic if and only if $C \cap D = \emptyset$.*

iii) *g is elliptic if and only if $C \cap D$ intersect in $\mathbb{H}$.*

Proof: Let $1 \neq g \in PGL_2(\mathbb{F})$.

Case 1. g is parabolic.

Working in the plane model, we may assume $g(\infty) = \infty$ so that $g(z) = z+b$, $b \in \mathbb{F}$. Let $C = \mathbb{I}+\frac{b}{2}$, $D = \mathbb{I}$. Then C and D are tangent at ∞ (and $r_{\mathbb{I}+\frac{b}{2}}(z) = -\overline{z}+b$, $r_{\mathbb{I}}(z) = -\overline{z}$).

Case 2. g is hyperbolic.

Working in the plane model, we may assume $g(\infty) = \infty$ and $g(0) = 0$ so that $g(z) = az$. Let $C = \{ z \mid z\overline{z} = a \}$ and $D = \mathbb{S}$. (Now $C \neq \emptyset$ since $a \in \mathbb{F}_+ \subseteq$

$\mathrm{Im}(N)$ if $g \in PSL_2(\mathbb{F})$ and N is onto otherwise.) Then $C \cap D = \emptyset$ (and $r_C(z) = \frac{a}{\bar{z}}, r_D(z) = \frac{1}{\bar{z}}$).

Case 3. g is elliptic.

Since $\mathbb{F} \subseteq \mathbb{E}_+$, g has two fixed points. Working in the disk model, we may assume these points are $0, \infty$. Then $g(z) = sz,\ s \in \mathbb{S}$ (by Lemma 3.10(ii)). Let $C = (s+1)\mathbb{F},\ D = \mathbb{F}$. So $C \cap D = \{0, \infty\}$ (and $r_C(z) = s\bar{z},\ r_D(z) = \bar{z}$).

Conversely, let $1 \neq g = r_C r_D$ with C and D hyperbolic mirrors. We may assume $C = \{\ z \in \mathbb{E} \mid z\bar{z} = a\bar{a}\ \}$ and $D = \{\ z \in \mathbb{E} \mid |z-1|^2 = b\bar{b}\ \}$ or $D = \{\ z \in \mathbb{E} \mid z\bar{z} = b\bar{b}\ \}$. Since $g \neq 1, C \neq D$. If C and D are concentric, then $C \cap D = \emptyset$ and $r_C r_D(z) = \left(\dfrac{a\bar{a}}{b\bar{b}}\right) z$ is in $\mathbb{F}^\times z$ and is hyperbolic. Otherwise, $r_D(z) = \dfrac{b\bar{b}}{\bar{z}-1} + 1$ and $r_C \circ r_D(z) = \dfrac{a\bar{a}(z-1)}{z + (b\bar{b}-1)}$.

Now $r_C \circ r_D(z) = z$ iff $z^2 + (b\bar{b} - a\bar{a} - 1)z + a\bar{a} = 0$. According to the classification of elements of $PGL_2(\mathbb{F})$, $r_C \circ r_D$ is hyperbolic iff $\triangle \in \mathbb{F}_+$, parabolic iff $\triangle = 0$ and elliptic iff $\triangle \in \mathbb{F}^\times - \mathbb{F}_+$ where $\triangle$ is the discriminant of the quadratic $z^2 + (b\bar{b} - a\bar{a} - 1)z + a\bar{a}$.

On the other hand, $z \in C \cap D$ iff $z\bar{z} = a\bar{a}$ and $(z-l)(\bar{z}-1) = z\bar{z} - z - \bar{z} + 1 = b\bar{b}$. Together these equations imply $a\bar{a} - b\bar{b} + 1 = z + \bar{z}$ and thus $z^2 + (b\bar{b} - a\bar{a} - 1)z + a\bar{a} = 0$ ($\bar{z} = \frac{a\bar{a}}{z}$ since $z \neq 0$). Consequently, C, D intersect at two points in $\mathbb{H}$ iff $\triangle \in \mathbb{F}^\times - \mathbb{F}_+$. From the equation $a\bar{a} - b\bar{b} + 1 = z + \bar{z}$, we see that C and D intersect in at most one point ($z = \dfrac{a\bar{a} - b\bar{b} + 1}{2}$) in $\mathbb{F}$. Thus, C and D intersect in exactly one point in $\mathbb{F}$ iff $\triangle = 0$ and are disjoint iff $\triangle \in \mathbb{F}_+$. $\square$

Remark: Let $g = r_C r_D$ where C, D are hyperbolic mirrors and $\mathbb{F} \subseteq \mathbb{E}_+$. If

g is elliptic, let C and D be as in the above proof. Then $g(z) = sz$ and $\det(g) = s$. Also $\mathrm{den}(D,C) = \mathrm{den}(\mathbb{F}, (s+1)\mathbb{F}) = s$. Consequently, $g \in PSL_2(\mathbb{F})$ if and only if $\mathrm{den}(D,C) \in \mathbb{S}_+$. If g is parabolic, then g is always in $PSL_2(\mathbb{F})$.

The hypothesis that $\mathbb{F} \subseteq \mathbb{E}_+$ in the above theorem was used to guarantee that all elliptic elements of $PGL_2(\mathbb{F})$ have fixed points. We now propose another way of fixing this problem. We define

$$\mathbb{U} := \{ \alpha \in \overline{\mathbb{F}} - \mathbb{F} \mid \dim_{\mathbb{F}} (\mathbb{F}[\alpha]) = 2 \}.$$

$PGL_2(\mathbb{F})$ (and $PSL_2(\mathbb{F})$) acts on $\mathbb{P}^1_{\overline{\mathbb{F}}} = \overline{\mathbb{F}} \cup \{\infty\} = (\overline{\mathbb{F}} - \mathbb{F}) \cup \mathbb{P}^1_{\mathbb{F}}$ with orbits $\mathbb{U}$ and $\mathbb{P}^1_{\mathbb{F}}$. $\mathbb{U}$ provides an alternate model for the hyperbolic plane in which all elliptic elements have fixed points. If $\mathbb{F}$ has a unique quadratic extension (e.g., $\mathbb{F} = \mathbb{R}$ or $\mathbb{F} = \mathbb{F}_q$) then $\mathbb{U} = \mathbb{E} - \mathbb{F} = \mathbb{H}$.

Theorem 3.20. *Let $a \neq b \in \mathbb{H}$.*

i) *There is a hyperbolic reflection fixing a and b which is unique if $a \neq \overline{b}$.*

ii) *If $g \in Isom(\mathbb{H},\Delta')$ fixing a and b and $a \neq \overline{b}$, then g is a hyperbolic reflection.*

Proof: If $a + \overline{a} = b + \overline{b}$, then we may assume $a + \overline{a} = b + \overline{b} = 0$. Then $r_{\mathbb{I}}(z) = -\overline{z}$ fixes a and b and has mirror $\mathbb{I}$. Otherwise, the line ab is not vertical and thus is not perpendicular to $\mathbb{F}$. Let L be the perpendicular bisector of ab. Then by Lemma 1.9(iii), $L \cap \mathbb{F} \neq \emptyset$. Translating if necessary, we may assume $L \cap \mathbb{F} = \{0\}$. By SDS, $\triangle(0, \frac{a+b}{2}, a) \cong \triangle(0, \frac{a+b}{2}, b)$ and thus $a\overline{a} = b\overline{b}$. Then $a, b \in C = \{ z \in \mathbb{E} \mid z\overline{z} = a\overline{a} \}$ and r_C is the desired hyperbolic isometry since the center 0 of C lies on $\mathbb{F}$.

Let $g = r_{\mathbb{I}}$ if $a+\overline{a} = b+\overline{b}$ and $g = r_C$ otherwise. If $a \neq \overline{b}$ and h is a hyperbolic isometry fixing a and b, then $h^{-1}g \in PGL_2(\mathbb{F})$ by Lemma 3.15. Then $h^{-1}g$ fixes $a, b, \overline{a}$ and is therefore 1. Therefore, $g = h$. This argument proves both ii) and the uniqueness of g in i). □

Given $a \neq b \in \mathbb{H}$, there is a hyperbolic mirror passing through a and b by Theorem 3.20(i). If $a \neq \overline{b}$, this hyperbolic mirror is unique and is denoted $M(a,b)$. The analogous statement holds for $x \neq y \in \mathbb{D}$.

Lemma 3.21. *Let $A, B \in \mathbb{D}$ with $0A \neq 0B$ and $B \neq \frac{1}{\overline{A}}$. Let $G = \{ z \mid |z-T|^2 = |B-T|^2 \}$ be the unique Euclidean circle such that $A, B \in G$ and G is a hyperbolic mirror of $\mathbb{D}$. Then*

$$T = \frac{B - A - B\overline{B}A + BA\overline{A}}{B\overline{A} - \overline{B}A}.$$

Proof: Now $|B-T|^2 = |A-T|^2 = T\overline{T} - 1$ since G is a hyperbolic mirror.

$$(B-T)(\overline{B-T}) = (A-T)(\overline{A-T}) = T\overline{T}-1 \implies B\overline{B}-\overline{B}T-B\overline{T} = A\overline{A}-\overline{A}T-A\overline{T} = -1.$$

Multiplying equation $B\overline{B}-\overline{B}T-B\overline{T} = -1$ by A and equation $A\overline{A}-\overline{A}T-A\overline{T} = -1$ by $-B$, we get

$$B\overline{B}A - \overline{B}AT - BA\overline{T} = -A, \quad -BA\overline{A} + B\overline{A}T + BA\overline{T} = B.$$

Adding these two equations gives

$$T(B\overline{A} - \overline{B}A) = B - A - B\overline{B}A + BA\overline{A}.$$

Since den$(0B,0A) \neq 1$, $B\overline{A} \notin \mathbb{F}$. □

Since isometries preserve orthogonality, the image of any hyperbolic mirror under an isometry is again a hyperbolic mirror. (Two such hyperbolic mirrors are said to be **isometric.**) Also $PGL_2(\mathbb{F})$ preserves the dengle between any two intersecting hyperbolic mirrors.

Consider the finite case with $\mathbb{F} = \mathbb{F}_q$. Hyperbolic mirrors of $\mathbb{H}$ which are vertical lines or circles centered on $\mathbb{F}$ and intersecting $\mathbb{F}$ have cardinality $q-1$, while the hyperbolic mirrors that are circles centered on $\mathbb{F}$ but not intersecting $\mathbb{F}$ have cardinality $q+1$. In particular, the classical result that all hyperbolic mirrors are isometric does not hold.

Lemma 3.22. *Let L and M be hyperbolic mirrors of $\mathbb{D}$ with $A, B \in L$ and $\triangle(A,B) \in \mathbb{F}^\times - \{-1\}$. L is isometric to M if and only if there exists $P, Q \in M$ with $\triangle(P,Q) = \triangle(A,B)$.*

Proof: If $g \in \mathrm{Isom}(\mathbb{D},\triangle)$ such that $g(L) = M$, then $\triangle(g(A), g(B)) = \triangle(A,B)$. Conversely, if there exists $P, Q \in M$ with $\triangle(PQ,=)\triangle(A,B)$, then there exists $g \in PGL_2(\mathbb{F})$ such that $g(P) = A$ and $g(Q) = B$. Since there is a unique hyperbolic mirror through any two distinct nonconjugate points and $A, B \in L \cap g(M)$, $g(M) = L$. $\square$

If follows from Lemma 3.22 that hyperbolic mirrors L and M are isometric if and only if they are isometric by an element of $PGL_2(\mathbb{F})$.

Theorem 3.23. *Let $A, B, P, Q \in \mathbb{D}$ with $d = \triangle(A,B)$, $\tilde{d} = \triangle(P,Q) \in \mathbb{F}^\times - \{-1\}$. $M(A,B)$ and $M(P,Q)$ are isometric if and only if $\frac{d}{d+1}$ and $\frac{\tilde{d}}{\tilde{d}+1}$ are in the same coset of $\mathbb{F}_+$ in $Im(N)$.*

Proof: Since U acts transitively on $\mathbb{D}$, we may assume $A = P = 0$. Since $B \in \{ z \in \mathbb{D} \mid \triangle(z,0) = d \} = \{ z \in \mathbb{E} \mid z\overline{z} = \frac{d}{d+1} \}$, $\frac{d}{d+1} \in \mathrm{Im}(N)$. Thus, the cosets $\left(\frac{d}{d+1}\right)\mathbb{F}_+$, $\left(\frac{\tilde{d}}{\tilde{d}+1}\right)\mathbb{F}_+$ are defined. Now $d = \triangle(B,0) = \frac{B\overline{B}}{1-B\overline{B}}$ and $\frac{d}{d+1} = B\overline{B}$. Note that

$$\triangle(rB,tB) \;=\; \frac{B\overline{B}(r-t)^2}{(1-r^2B\overline{B})(1-t^2B\overline{B})},\quad \triangle(\infty,tB) \;=\; \frac{-1}{1-t^2B\overline{B}}$$

for $r,t \in \mathbb{F}$. Since $M(A,B) = \widehat{B\mathbb{F}}$,

$M(P,Q)$ is isometric to $M(A,B)$

$$\iff \tilde{d} = \triangle(rB,tB) \;\text{ or }\; \tilde{d} = \triangle(\infty,tB) \text{ for some } r,t \in \mathbb{F}$$

$$\iff \frac{\tilde{d}}{\tilde{d}+1} = \frac{B\overline{B}(r-t)^2}{(rtB\overline{B}-1)^2} \;\text{ or }\; \frac{\tilde{d}}{\tilde{d}+1} = \frac{1}{t^2B\overline{B}} \text{ for some } r,t \in \mathbb{F}.$$

Also

$$\left(\frac{d}{d+1}\right)\mathbb{F}_+ \;=\; \left(\frac{\tilde{d}}{\tilde{d}+1}\right)\mathbb{F}_+ \;\iff\; \frac{d}{d+1} = x^2\left(\frac{\tilde{d}}{\tilde{d}+1}\right) \text{ for some } x \in \mathbb{F}^\times.$$

If $M(P,Q)$ is isometric to $M(A,B)$, then $B\overline{B} = x^2\left(\frac{\tilde{d}}{\tilde{d}+1}\right)$ where $x = \frac{rtB\overline{B}-1}{(r-t)^2}$ or $x = t^2(B\overline{B})^2$ for some $r,t \in \mathbb{F}$.

Conversely, if $B\overline{B} = x^2\left(\frac{\tilde{d}}{\tilde{d}+1}\right)$ for some $x \in \mathbb{F}^\times$, then $\tilde{d} = \frac{B\overline{B}}{x^2-Q\overline{Q}} = \triangle(\left(\frac{1}{x}\right)Q,0)$. $\square$

Corollary 3.24. *The number of $PGL_2(\mathbb{F})$ orbits of hyperbolic mirrors in $\mathbb{D}$ is $[\, Im(N) : \mathbb{F}_+]$.*

In particular, there are two isometry classes of hyperbolic mirrors in the finite case.

Lemma 3.25. *Let G be a hyperbolic mirror in $\mathbb{D}$, $p \in G$, $s \in \mathbb{S}$. There is a unique hyperbolic mirror H with $p \in H$ and den(G,H,p) $= s$.*

Proof: We may assume $P = 0$. Then G is an extended line and the result follows from Lemma 1.12. $\square$

Proposition 3.26. *Let $P \neq Q \in C \cap W$ where $C = \{ z \in \mathbb{D} \mid \triangle(z, A) = \lambda \}$, $W = \{ z \in \mathbb{D} \mid \triangle(z, B) = \mu \}$, $A \notin \{B, \overline{B}\}$ and $\lambda, \mu \in \mathbb{F}^{\times} - \{-1\}$. If M is any hyperbolic mirror through P and Q and $L = M(A, B)$, then $L = \{ z \in \mathbb{D} \mid \triangle(z, P) = \triangle(z, Q) \}$, $L \ \Psi \ M$ and $r_L(P) = Q$.*

Proof: We may assume $A = 0$. Then $L = \widehat{0B}$. Since $\triangle(0, P) = \triangle(0, Q)$ and $\triangle(B, P) = \triangle(B, Q)$, $0B \perp PQ$. Thus,

$$\{ z \in \mathbb{D} - \{\infty\} \mid \triangle(z, P) = \triangle(z, Q) \} = \{ z \in \mathbb{D} - \{\infty\} \mid 0z \perp PQ \} = 0B$$

and $L = \{ z \in \mathbb{D} \mid \triangle(z, P) = \triangle(z, Q) \}$. Since $r_L(P) \in C \cap W = \{P, Q\}$ and $P \notin L$, $r_L(P) = Q$.

If $0 \in M$, then M is an extended line. Since $P\overline{P} = Q\overline{Q}$, $0B$ is the perpendicular bisector of PQ and thus $L \ \Psi \ M$ and $r_L(P) = Q$. If $0 \notin M$, then let R be the Euclidean center of M. If $R \neq 0$, then by Lemma 1.32(ii) $0R$ is the perpendicular bisector of PQ. Since $0B \perp PQ$ we have $0B = 0R$. In any case, $R \in L$ and thus $L \ \Psi \ M$. $\square$

Proposition 3.27. *Assume $\mathbb{F} \neq \mathbb{F}_3$.*

i) *If G is a hyperbolic mirror in $\mathbb{D}$ with $p \in G$, there is a unique hyperbolic mirror passing through p and orthogonal to G.*

ii) *Given $p \in \mathbb{D}$, there is a unique hyperbolic mirror T_p such that every hyperbolic mirror through p is orthogonal to T_p. Moreover, if $H \neq T_p$ is a hyperbolic mirror, then there's a unique hyperbolic mirror through p and orthogonal to $\mathbb{H}$.*

Proof: We may assume $p = 0$.

i) Every hyperbolic mirror through 0 is an extended line. Thus, given any hyperbolic mirror G with $0 \in G$, there's a unique line passing through 0 and perpendicular to G.

ii) By i), it suffices to consider a hyperbolic mirror G with $0 \notin G$. Then G is a Euclidean circle with Euclidean center R. If $R \neq 0$, then the unique hyperbolic mirror passing through 0 and orthogonal to G is $0R$. There is a unique circle with $R = 0$ which is a hyperbolic mirror, namely T. But every hyperbolic mirror passing through 0 is orthogonal to T. $\square$

Question: Given disjoint hyperbolic mirrors G and H, when do they have a (necessarily unique) common orthogonal?

Assume $\mathbb{F} \neq \mathbb{F}_3$. Working in the $\mathbb{H}$ model, we may assume G and H are circles centered on $\mathbb{F}$. If G and H are concentric with center t, then the unique common orthogonal is the vertical line passing through t (by Proposition 2.16). Otherwise, the only possible common orthogonal to G and H is the circle K with center $\dfrac{a^2 - b^2 - \lambda + \mu}{2(a-b)}$ and sqradius $\eta = \left(\dfrac{(a-b)^2 + \lambda - \mu}{2(a-b)}\right)^2 - \lambda$ where G has center a, $\mathrm{sqr}(\lambda)$ and H has center b, $\mathrm{sqr}(\mu)$ (again by Proposition 2.16). It is not clear from the formulas that K is nonempty. Specifically, why is

η nonzero and in the image of the norm map?

To make computations easier, we will further assume that $a = 0$ and $b = 1$. Since G and H are disjoint, $r_G r_H(z) = \dfrac{\lambda z - \lambda}{z + (\mu - 1)}$ is hyperbolic (Theorem 3.19) with fixed points $z = \dfrac{1 + \lambda - \mu \pm \delta}{2} \in \mathbb{F}$ where $\delta^2 = (\mu - \lambda - 1)^2 - 4\lambda \in \mathbb{F}_+$.

Claim. *The fixed points of $r_G r_H$ lie on K.*

Proof: We need to show that

$$\left| \frac{1 + \lambda - \mu}{2} - z \right|^2 = \frac{(1 + \lambda - \mu)^2}{4} - \lambda.$$

Let $x = 1 + \lambda - \mu$. Then $z = \dfrac{x \pm \delta}{2}$ and $\delta^2 = x^2 - 4\lambda$. Therefore,

$$\left| \frac{1 + \lambda - \mu}{2} - z \right|^2 = \left| \frac{x}{2} - z \right|^2 = \left(\frac{x}{2} - z \right)^2 = \frac{x^2}{4} - xz + z^2,$$

$$\frac{(1 + \lambda - \mu)^2}{4} - \lambda = \frac{x^2}{4} - \lambda.$$

But $z^2 - xz = \left[\dfrac{(x \pm \delta)}{2} \right]^2 - x \left(\dfrac{x \pm \delta}{2} \right) = \dfrac{x^2 \pm 2\delta + \delta^2 - 2x^2 \mp 2\delta x}{4} = \dfrac{\delta^2 - x^2}{4} = \dfrac{x^2 - 4\lambda - x^2}{4} = -\lambda$. $\square$

Corollary 3.28. *If G and H are disjoint hyperbolic mirrors, then the unique hyperbolic mirror passing through the fixed points of $r_G r_H$ is a common orthogonal of G and H.*

Corollary 3.29. *If G and H are disjoint hyperbolic mirrors, then G and H are conjugate to two concentric circles.*

Proof: Since $r_G r_H$ is hyperbolic, its fixed points lie on $\widehat{\mathbb{F}}$ and thus the common orthogonal of G and H intersects $\mathbb{F}$. Thus, we may assume the common orthogonal is $\mathbb{I} \cup \{0\}$ which implies that G and H are both circles centered at 0. $\square$

Unlike the classical case, it is also possible for G and H to have a common orthogonal even if they are not disjoint. For example, let $\mathbb{F} = \mathbb{F}_5$ and α be a root of the quadratic $x^2 + 2$, irreducible over $\mathbb{F}_5$. Let G be the vertical line through $2 \pm \alpha$ and $H = \mathbb{S}$. Then $G \cap H = \{2 \pm \alpha\}$ and the circle centered at 2 with sqradius -2 is the common orthogonal.

Theorem 3.30. *If G and H are hyperbolic mirrors intersecting in $\mathbb{H}$ and $-1 \in Im(N)$, then T is a common orthogonal of G and H.*

Proof: Working in the disk model, we may assume the fixed points of $r_G r_H$ are 0 and ∞ (since $r_G r_H$ is elliptic by Theorem 3.19). Then G and H are extended lines passing through 0 and both are orthogonal to T when T exists. $\square$

In the finite case for instance, there are therefore three possibilities for distinct hyperbolic mirrors G and H:

i) If G and H are disjoint, they have a unique common orthogonal intersecting $\mathbb{F}$ (and conjugate to $\mathbb{I} \cup \{0\}$).

ii) If G and H intersect in $\mathbb{H}$, they have a unique common orthogonal not intersecting $\widehat{\mathbb{F}}$ (and conjugate to T).

iii) If G and H intersect in $\widehat{\mathbb{F}}$, they do not have a common orthogonal. (Conjugate so that G and H are vertical lines.)

Definition: Distinct hyperbolic mirrors G and H will be called **parallel** if they intersect in $\widehat{\mathbb{F}}$.

Theorem 3.31. *Every hyperbolic element of $PGL_2(\mathbb{F})$ can be written as a product of two hyperbolic reflections if and only if the norm map is onto.*

Proof: Let $a \in \mathbb{F}^\times$. Then $g(z) = az$ is hyperbolic. If $g(z) = r_G r_H$, then G and H are disjoint mirrors having common orthogonal $\mathbb{I} \cup \{0\}$. But $r_G r_H(z) = \left(\frac{\lambda}{\mu}\right) z$ where λ is the sqradius of G and μ is the sqradius of H. Since λ and μ are in Im(N) and N is a group homomorphism from a multiplicative group, we have $a = \frac{\lambda}{\mu} \in$ Im(N). Hence, N is onto.

The converse was proved in Theorem 3.17. □

For instance, $z \mapsto -z$ is not a product of two hyperbolic reflections when $\mathbb{F} = \mathbb{R}$.

Even though disjoint hyperbolic mirrors G and H have a common orthogonal K, K may intersect neither G nor H. (If G and H are concentric circles centered at 0, $K = \mathbb{I}$ may not touch either circle.) Nevertheless, if G and H are disjoint hyperbolic mirrors having a common perpendicular K, then we can recover some of the classical theory. We can, for instance, define the distance between G and H in this case.

Definition: Let C and D be disjoint hyperbolic mirrors with a common perpendicular K such that $K \cap C = \{P\}$, $K \cap D = \{Q\}$. Change coordinates so that $P = 0$. Then $C = c\mathbb{F}$, D is a circle centered at $A \in \mathbb{E}$ satisfying sqr(D) $= A\overline{A} - 1$ and $K = 0A$. We define the **hyperbolic distance from** C **to** D **at** Q as follows:

$$\triangle(C, D, Q) := \triangle(0, Q) = \frac{Q\overline{Q}}{1 - Q\overline{Q}}.$$

Moreover, $\cosh(\triangle(C,D,Q)) := 1 + 2\triangle(C,D,Q)$.

Given a field $\mathbb{K}$, consider the map from $GL_n(\mathbb{K})$ into $\mathbb{K}$ given by $A \longmapsto \frac{(tr(A))^n}{det(A)}$. Given $\lambda \in \mathbb{K}^\times$, $\mathrm{tr}(\lambda A) = \lambda \mathrm{tr}(A)$ and $\det(\lambda A) = \lambda^n \det(A)$. I.e., the map $A \longmapsto \frac{(tr(A))^n}{det(A)}$ factors through $PGL_n(\mathbb{K})$. Let $\phi_n : PGL_n(\mathbb{K}) \longrightarrow \mathbb{K}$ be the induced map.

Since both the trace and the determinant of a matrix are invariant under conjugation, $\phi_n(\alpha) = \phi_n(\beta)$ when α and β are conjugate in $PGL_2(\mathbb{K})$.

Definition: The **inversive product** of hyperbolic mirrors C and D is $\phi_2(r_C \circ r_D)$ and is denoted (C, D).

Lemma 3.32. *Let $\alpha = [A]$, $\beta = [B]$ be nonidentity elements of $PGL_2(\mathbb{K})$.*

i) *If $\phi_2(\alpha) \neq 0$, then β is conjugate to α in $PGL_2(\mathbb{K})$ if and only if $\phi_2(\alpha) = \phi_2(\beta)$.*

ii) *If $\phi_2(\alpha) = 0$, then β is conjugate to α in $PGL_2(\mathbb{K})$ if and only if $\phi_2(\alpha) = \phi_2(\beta)$ and $\frac{\det(A)}{\det(B)} \in \mathbb{K}_+$.*

Proof: Note that $\det(A) = \det(\lambda B) = \lambda^2 \det(B)$ for some $\lambda \in \mathbb{K}_+$ if and only if $\frac{\det(A)}{\det(B)} \in \mathbb{K}_+$.

i) Assume $\frac{tr^2(A)}{det(A)} = \frac{tr^2(B)}{det(B)}$. Then $\frac{det(A)}{det(B)} = \frac{tr^2(A)}{tr^2(B)} \in \mathbb{K}_+$ and we can find a representative $\widetilde{B}$ of α with $\det(A) = \det(\widetilde{B})$. Consequently, $\phi_2(\alpha) = \phi_2(\beta)$ implies $tr^2(A) - 4\det(A) = tr^2(\widetilde{B}) - 4\det(\widetilde{B})$. I.e, α and β are conjugate in $PGL_2(\mathbb{K})$ by Proposition 0.5.

ii) Since $\frac{\det(A)}{\det(B)} \in \mathbb{K}_+$, we can find a representative $\widetilde{B}$ of β with $\det(A) =$

$\det(\widetilde{B})$. Since $tr^2(A) = 0 = tr^2(\widetilde{B})$, α and β are conjugate in $PGL_2(\mathbb{K})$ by Proposition 0.5. $\square$

Let $\mathbb{K} = \mathbb{F}_5$. Then $\mathbb{K}_+ = \{\pm 1\}$. Consider $g(z) = \frac{-1}{z}$ and $h(z) = \frac{-2}{z}$. Then $tr^2(g) = 0 = tr^2(h)$ but g and h are not conjugate in $PGL_2(\mathbb{K})$ since $\det(g) = 1 \in \mathbb{K}_+$ but $\det(h) = 2 \notin \mathbb{K}_+$.

Theorem 3.33. *Let C and D be distinct hyperbolic mirrors of $PSL_2(\mathbb{F})$. Then*

i) *If $C \cap D = \{P\}$, then $(C,D) = 4\cos^2(\gamma)$ where γ = den(C,D,P).*

ii) *If C and D are disjoint and have a common perpendicular $\mathbb{K}$, then $(C,D) = 4\cosh^2(\Delta(C,D,Q))$ where $Q \in D \cap \mathbb{K}$.*

Proof: i) By a change of coordinates we may assume $C = \lambda\mathbb{S}$ and $D = \mu\mathbb{S} + d$, $d \in \mathbb{F}$. Then

$$\begin{aligned} r_C \circ r_D &= \frac{\lambda(z-d)}{\bar{d}z + (\mu - d\bar{d})}, \\ (C,D) &= \phi_2\left(\begin{bmatrix} \lambda & -\lambda d \\ \bar{d} & \mu - d\bar{d} \end{bmatrix}\right) = \frac{(\lambda + \mu - d\bar{d})^2}{\lambda\mu}. \end{aligned}$$

On the other hand, applying the Law of Cosines (Proposition 1.56) to $\Delta(0,P,d)$ gives $(\lambda + \mu - d\bar{d})^2 = 4\lambda\mu\cos^2(\gamma)$ where $\gamma = \text{den}(0P,\ Pd)$. Hence,

$$(C,D) = 4\cos^2(\gamma) = \left(\frac{\gamma+1}{\gamma}\right)^2$$

where γ = den(C,D,P).

ii) If $C \cap D = \emptyset$, change coordinates so that $C = c\mathbb{F}$, D is a circle centered at $d \in \mathbb{E}$ satisfying $\text{sqr}(D) = d\bar{d} - 1$, $\mathbb{K} = 0d$. Now $r_C(z) = \frac{c}{\bar{c}}\bar{z}$, $r_D(z) = \dfrac{d\bar{z} - 1}{\bar{z} - \bar{d}}$. Therefore,

$$r_C r_D(z) = \frac{c}{\bar{c}}\left[\frac{\bar{d}z - 1}{z - d}\right].$$

Since $Q \in 0d = Q\mathbb{F}$, $d = aQ$ for some $a \in \mathbb{F}$. Therefore, $\mathrm{sqr}(D) = |Q - d|^2 = d\bar{d} - 1 \implies Q\overline{Q} - d\overline{Q} - \bar{d}Q = -1 \implies Q\overline{Q} - 2Q\overline{Q}a = -1 \implies a = \dfrac{Q\overline{Q}+1}{2Q\overline{Q}}$ and $d = \dfrac{Q\overline{Q}+1}{2\overline{Q}}$. Thus,

$$r_C r_D(z) = \frac{c\overline{Q}}{\bar{c}Q}\left[\frac{(Q\overline{Q}+1)z - 2Q}{2\overline{Q}z - (Q\overline{Q}+1)}\right].$$

Since $\dfrac{C\overline{Q}}{\overline{C}Q} = \mathrm{den}(0C{,}0Q) = \mathrm{den}(C{,}K) = \text{-}1$, we have $\phi(r_C \circ r_D) = \dfrac{4(Q\overline{Q}+1)^2}{(Q\overline{Q}-1)^2}$.
But $1 + 2\triangle(C, D, Q) = 1 + 2\left[\dfrac{Q\overline{Q}}{1 - Q\overline{Q}}\right] = \dfrac{1+Q\overline{Q}}{1-Q\overline{Q}}$. $\square$

Remarks: i) If $C \cap D \neq \emptyset$, then the proof of part i) of the above theorem shows that $(C, D) = \dfrac{(\lambda + \mu - d\bar{d})^2}{\lambda\mu}$. Thus, $r_C \circ r_D \in PSL_2(\mathbb{F})$ iff $\det(r_C \circ r_D) \in \mathbb{F}_+$ iff $(C, D) \in \mathbb{F}_+$ iff $\lambda\mu \in \mathbb{F}_+$.

ii) It follows from Theorem 3.33(ii) that $\cosh^2(\triangle(C, D, Q)) = \cosh^2(\triangle(C, D, \widetilde{Q}))$ where $\{Q, \widetilde{Q}\} = K \cap D$. I.e.,

$$\triangle(0, Q) + \triangle(0, \widetilde{Q}) = -1.$$

Definition: $A, B, C \in \mathbb{H}$ are **cocyclic in** $\mathbb{H}$ if there is a hyperbolic mirror of $\mathbb{H}$ containing A, B, C.

Definition: Let A, B, C be noncyclic points of $\mathbb{H}$. The **hyperbolic triangle** with vertices A, B and C is $M(A, B) \cup M(B, C) \cup M(C, A)$ and is denoted ABC.

Mirrors $M(A, B)$, $M(B, C)$, $M(C, A)$ are the **sides** of the triangle.

The oriented triangle (A, B, C) is the triangle ABC with dengles den($M(A, B)$, $M(B, C)$, B), den($M(B, C)$, $M(C, A)$, C), and den($M(C, A)$, $M(A, B)$, A).

Note that no two vertices of a triangle are conjugate. (If $B = \overline{A}$, then $B \in M(A, C)$.)

Triangles ABC and PQR are **isometric** (denoted $ABC \cong PQR$) if there is a g in Isom($\mathbb{H}$, Δ') such that $g(A) = P$, $g(B) = Q$, $g(C) = R$ and **weakly isometric** (denoted $ABC \cong_W PQR$) if there is an h in Isom($\mathbb{H}$, Δ') such that $h(M(A,B)) = M(P,Q)$, $h(M(B,C)) = M(Q,R)$, $h(M(C,A)) = M(R,P)$.

(A, B, C) is a **right triangle** if (at least) one of its dengles is -1.

Lemma 3.34. *Consider* (A, B, C).

i) *den(* $M(B,C)$, $M(C,A)$, C *)* $= -1 =$ *den(* $M(C,A)$, $M(A,B)$, A *) if and only if* $A, C \in T$.

ii) *If den(* $M(B,C)$, $M(C,A)$, C *)* $= -1$, *then* $\Delta(B,C) = \Delta(A,B)$ *if and only if* $A, C \in T$.

Proof: We may assume $B = 0$. Then $M(A, 0) = \widehat{OA}$, $M(0, C) = \widehat{0C}$ and $M(A, C)$ is a Euclidean circle with center R.

i) Now den($\widehat{0C}$, $M(C,A)$, C) $= -1 =$ den($M(C,A)$, $\widehat{0A}$, A) if and only if $R \in (0C) \cap (0A) = \{0\}$ if and only if $M(A,C) = T$.

ii) Since den($\widehat{0C}$, $M(C,A)$, C) $= -1$, $r_{0C}(M(C,A)) = M(C,A)$. Let $W = \{ z \in \mathbb{D} \mid \Delta(0,z) = \Delta(0,A) \}$, a Euclidean circle centered at 0. Note that $r_{0C}(A) \in W \cap M(C,A)$ and $r_{0C}(A)$, A, C are distinct. Consequently, $\Delta(0,C) = \Delta(A,0) \iff C \in W \iff W = M(C,A) \iff M(C,A) = T$. $\square$

Proposition 3.35. *In* (A, B, C), $\Delta(A,B) = \Delta(A,C)$ *if and only if* $\beta = \tau$ *where* $\beta =$ *den(*$M(A,B)$, $M(B,C)$, B*) and* $\tau =$ *den(*$M(B,C)$, $M(A,C)$, C*).*

Proof: We may assume $A = 0$. Then $M(0,B) = \widehat{0B}$, $M(0,C) = \widehat{0C}$ and $M(B,C)$ is a Euclidean circle centered at R.

If $R = 0$, then $M(B,C) = T$ and both $\Delta(0,B) = \Delta(0,C)$ and $\beta = \tau = -1$ hold. Assume $R \neq 0$. Let $L = 0R$. Note that $r_L(M(B,C)) = M(B,C)$, that $B, r_L(B), C \in G$ and that $B, r_L(B) \in W = \{ z \in \mathbb{D} \mid \Delta(0,z) = \Delta(0,B) \}$. Since $G \neq W$, $\Delta(0,B) = \Delta(0,C) \iff C \in W \iff r_L(B) = C$. (Since $r_L(C) \in G \cap W$ when $C \in W$, $r_L(B) = B$ implies that $r_L(C) = C$ and 0, B, C are collinear.)

Now $\beta =$ den($\widehat{0B}$, $M(B,C)$, B) and $\tau =$ den($M(B,C)$, $\widehat{0C}$, C). Thus, $\frac{1}{\beta}$ $=$ den($\widehat{0r_L(B)}$, $M(B,C)$, $r_L(B)$) and $\frac{1}{\tau} =$ den($\widehat{0C}$, $M(B,C)$, C).

If $r_L(B) = C$, then $\frac{1}{\beta} =$ den($\widehat{0C}$, $M(B,C)$, C) $= \frac{1}{\tau}$ and $\beta = \tau$. Conversely, assume $\beta = \tau$. If $r_L(B) \neq C$, then $r_L(r_L(0B)) = 0C$ by the Essential Uniqueness of Dengles Theorem. This can't happen since $0, B, C$ are not collinear. Thus, $\beta = \tau$ if and only if $r_L(B) = C$. $\square$

Proposition 3.36. *(SSS) If $\Delta(P,Q) = \Delta(A,B)$, $\Delta(Q,R) = \Delta(B,C)$ and $\Delta(R,P) = \Delta(C,A)$ in PQR and ABC, then $PQR \cong ABC$.*

Proof: We may assume $Q = B = 0$. Since $\Delta(0,P) = \Delta(0,A)$, there exists a $g \in U$ such that $g(0) = 0$, $g(A) = P$. Let

$$V = \{ z \in \mathbb{D} \mid \Delta(z,0) = \Delta(0,R) \}, \quad W = \{ z \in \mathbb{D} \mid \Delta(z,P) = \Delta(P,R) \}.$$

Since $V \neq W$ and $R, C \in V \cap W$, Proposition 3.26 implies that $R = C$ or $r_{0P}(C) = R$. In either case, $ABC \cong PQR$. $\square$

Proposition 3.37. *(SDS) If* $\triangle(A,B) = \triangle(P,Q)$, $\triangle(B,C) = \triangle(Q,R)$ *and* β $=$ *den(* $M(A,B)$, $M(B,C)$, B *)* $=$ *den(* $M(P,Q)$, $M(Q,R)$, Q *) in* (A,B,C) *and* (P,Q,R)*, then* (P,Q,R) *is isometric to either* (A,B,C) *or* (D,B,C) *where*

$$\{A \neq D\} = (AB) \cap \{\ z \in D \mid \triangle(z,B) = \triangle(A,B)\ \}.$$

If $\beta = -1$*, then* $(P,Q,R) \cong (A,B,C)$.

Proof: We may assume $B = Q = 0$. Since $\triangle(0,C) = \triangle(0,R)$, WMA $C = R$. Since den($0A$,$0C$) $=$ den($0P$,$0C$), we know $0A = 0P$.

Since $P \in (0A) \cap \{\ z \in \mathbb{D} \mid \triangle(z,0) = \triangle(A,0)\ \} = \{A,D\}$, $\triangle(P,Q,R) \cong \triangle(A,B,C)$ or $\triangle(P,Q,R) \cong \triangle(D,B,C)$. If $\beta = -1$, then $0A \perp 0C$ and

$$A, P, r_{0C}(A) \in (0A) \cap \{\ z \in \mathbb{D} \mid \triangle(z,0) = \triangle(A,0)\ \}.$$

Hence, $r_{0C}(A) = P$. $\square$

Proposition 3.38. *(DSS for right triangles)*

If den($M(B,C)$, $M(C,A)$, C *)* $= -1 =$ *den(* $M(Q,R)$, $M(R,P)$, R *),* $\triangle(A,B) = \triangle(P,Q)$, $\triangle(B,C) = \triangle(Q,R)$ *and* $\triangle(A,B) \neq \triangle(B,C)$ *in* (A,B,C) *and* (P,Q,R)*, then* $(A,B,C) \cong (P,Q,R)$.

Proof: We may assume $B = Q = 0$ and $C = R$. Since

$$den(\ \widehat{0C},\ M(A,C),\ C\ ) = den(\ \widehat{0C},\ M(P,C),\ C\ ),$$

we have $M(A,C) = M(P,C)$ by Lemma 3.25.

Now A, P, $r_{0C}(P) \in W = \{\ z \in \mathbb{D} \mid \triangle(z,0) = \triangle(0,A)\ \}$. Since den($\widehat{0C}$, $M(A,C)$, C) $= -1$, we know $A, P, r_{0C}(P) \in M(A,C)$. Since $\triangle(A,B) \neq \triangle(B,C)$, $W \neq M(A,C)$ and thus $r_{0C}(P) = A$. $\square$

Proposition 3.39. *(DSD)*

If den($M(A,B)$, $M(B,C)$, B) = den($M(P,Q)$, $M(Q,R)$, Q), den($M(B,C)$, $M(C,A)$, C) = den($M(Q,R)$, $M(R,P)$, R), and $\triangle(B,C) = \triangle(Q,R)$ in (A,B,C) and (P,Q,R), then (P,Q,R) is isometric to either (A,B,C) or $(\frac{1}{A},B,C)$.

Proof: We may assume $B = Q = 0$ and $C = R$. Since den($0A$,$0C$) = den($0P$,$0C$), $0A = 0P$. Also $M(C,A) = M(C,P)$ by Lemma 3.25 since

$$den\ \widehat{0C},\ M(C,A),\ C\ ) = den(\ \widehat{0C},\ M(C,P),\ C\ ).$$

Thus, $\widehat{0A}$ and $M(C,A)$ are distinct mirrors (since $0 \notin M(C,A)$) containing both A and P. Thus, $P = A$ or P is conjugate to A in $\mathbb{D}$. $\square$

Two triangles in $\mathbb{D}$ satisfying the data of DDS are not necessarily even weakly isometric.

Definition: Let $P_1, P_2, \ldots, P_n$ be distinct points (called **vertices**) of $\mathbb{H}$, no three of which are cocyclic in $\mathbb{H}$. The union of the mirrors $M(P_1,P_2), M(P_2,P_3), \ldots, M(P_{n-1},P_n)$, $M(P_n,P_1)$ (called **sides**) is a **hyperbolic n-gon**, denoted $P_1P_2\cdots P_n$.

$(P_1, P_2, \ldots, P_n)$ will denote the n-gon with dengles den($M(P_1,P_2)$,$M(P_2,P_3)$),..., den($M(P_{n-1},P_n)$,$M(P_n,P_1)$).

Proposition 3.40. *There is no rectangle in $\mathbb{D}$.*

Proof: Suppose (A,B,C,P) is a rectangle in $\mathbb{D}$. We may assume $P = 0$. Now $M(A,B)$ and $M(B,C)$ are Euclidean circles with centers Q, R respectively.

Thus,

$$|B-Q|^2 \;=\; Q\overline{Q}-1 \text{ and } |B-R|^2 \;=\; |C-R|^2 = R\overline{R}-1.$$

Consequently, $B\overline{B}-B\overline{Q}-\overline{B}Q = -1$ and $B\overline{B}-B\overline{R}-\overline{B}R = -1 = C\overline{C}-C\overline{R}-\overline{C}R$.

Since den($\widehat{0C}$, $M(B,C)$, C) = -1 = den($\widehat{0A}$, $M(A,B)$, A), we know $R \in 0C$ and $Q \in 0A$. Thus, den($0C$,$0R$) = $\dfrac{R\overline{C}}{\overline{C}\overline{R}}$ $= 1$ and $C\overline{R} = \overline{C}R$. Therefore,

$$C\overline{C}-2C\overline{R} \;=\; B\overline{B}-B\overline{R}-\overline{B}R \;=\; -1 \;=\; B\overline{B}-B\overline{Q}-\overline{B}Q.$$

Since den($0C$,$0A$) = den($0R$,$0Q$) $= -1$, we know $Q\overline{R} = -\overline{Q}R$. Since

$$-1 = den(M(A,B), M(B,C), B) = den(QB, BR),$$

$(B-R)(\overline{B-Q}) = -(B-Q)(\overline{B-R})$. Thus,

$$\begin{aligned} B\overline{B}-\overline{B}R-B\overline{Q}+\overline{Q}R \;&=\; -B\overline{B}+\overline{B}Q+B\overline{R}-\overline{R}Q \\ \Longrightarrow B\overline{B}-B\overline{Q}-\overline{B}Q \;&=\; -(B\overline{B}-B\overline{R}-\overline{B}R). \end{aligned}$$

In particular, $C\overline{C}-2C\overline{R} = B\overline{B}-B\overline{R}-\overline{B}R = B\overline{B}-B\overline{Q}-\overline{B}Q = -(B\overline{B}-B\overline{R}-\overline{B}R)$ and so $C\overline{C}-2C\overline{R} = 0$. This is a contradiction since $C = 2R$ implies that $|C-R|^2 = R\overline{R} \neq R\overline{R}-1$. □

Definition: The conjugate of the product of the dengles of the n-gon $(P_1P_2P_3\cdots P_n)$ is the **derea of** $(P_1P_2P_3\cdots P_n)$.

Lemma 3.41. *Assume $P \in M(B,C)-\{B,C\}$ in the triangle (A,B,C). Then the derea of (A,B,C) is the product of the derea of (A,B,P) and the derea of (A,P,C).*

Proof: We may assume $B = 0$. Then $M(A,C)$ and $M(A,P)$ are Euclidean circles with centers R,Q respectively.

Now the derea of (A,B,C) is the conjugate of

$$den(0A,0C)den(\widehat{0C},M(A,C),C)den(M(A,C),\widehat{0A},A)$$

$$= den(0A,0C)(-den(0C,CR))(-den(AR,0A))$$

$$= den(0A,CR)den(AR,0A) \;=\; den(AR,CR).$$

The derea of (A,B,P) is the conjugate of

$$den(0A,0P)den(\widehat{0P},M(A,P),P)den(M(A,P),\widehat{0A},A)$$

$$= den(0A,0P)(-den(0P,PQ))(-den(AQ,0A))$$

$$den(0A,PQ)den(AQ,0A) \;=\; den(AQ,PQ).$$

The derea of (A,P,C) is the conjugate of

$$den(M(A,P),\widehat{PC},P)den(\widehat{PC},M(A,C),C)den(M(A,C),M(A,P),A)$$

$$= \quad (-den(PQ,PC))(-den(PC,CR))(den(AR,AQ))$$

$$= \quad den(PQ,CR)den(AR,AQ).$$

Therefore,

$$den(AT,PQ)den(PT,CR)den(AR,AQ) \;=\; den(AQ,CR)den(AR,AQ)$$

$$= den(AR,CR). \quad \square$$

The analogue of Lemma 3.41 holds for any n-gon.

Consider $(A,B,0)$ in $\mathbb{D}$. Then $M(A,B)$ is a Euclidean circle with center R. Since $|A-R|^2 = |B-R|^2$, $\delta = \mathrm{en}(AR,BR)$ is defined. Recall that $[en(AR,BR)]^2$ $= \mathrm{den}(AR,BR)$. The derea of $(A,B,0)$ is the conjugate of

$$den(M(A,B),\widehat{0B},B)den(0B,0A)den(\widehat{0A},M(A,B),A)$$

$$= (-den(BR,0B)(den(0B,0A))(-den(0A,AR))$$

$$= den(BR,AR).$$

Thus, the derea of $(A,B,0)$ is $\overline{den(BR,AR)} = den(AR,BR) = \delta^2$.

Definition: The **erea** of $(A,B,0)$ is en(AR,BR) $= \dfrac{B-R}{A-R}$ where R is the Euclidean center of $M(A,B)$.

Hence, the derea of $(A,B,0)$ is the square of the erea of $(A,B,0)$.

Lemma 3.42. *The erea of* $(A,B,0)$ *is* $\dfrac{1-\overline{A}B}{1-A\overline{B}}$.

Proof: The erea of $(A,B,0) = \dfrac{R-B}{R-A}$ where R is the Euclidean center of $M(A,B)$. By Lemma 3.20, $R = \dfrac{A-B-A\overline{A}B+AB\overline{B}}{A\overline{B}-\overline{A}B}$. Therefore,

$$\begin{aligned} R-B &= \frac{A-B-A\overline{A}B+AB\overline{B}-AB\overline{B}+\overline{A}BB}{A\overline{B}-\overline{A}B} \\ &= \frac{A(1-\overline{A}B)-B(1-\overline{A}B)}{A\overline{B}-\overline{A}B} = \frac{(A-B)(1-\overline{A}B)}{A\overline{B}-\overline{A}B}. \end{aligned}$$

Similarly, $R-A = \dfrac{(A-B)(1-A\overline{B})}{A\overline{B}-\overline{A}B}$. Thus, $\dfrac{R-B}{R-A} = \dfrac{1-\overline{A}B}{1-A\overline{B}}$. □

Lemma 3.43. *The erea of* $(K(B),K(0),0)$ *and the erea of* $(A,B,0)$ *are equal where* $k(z) = \dfrac{z-A}{\overline{A}z-1}$.

Proof: Now $k(0) = A$ and $k(B) = \dfrac{B-A}{\overline{A}B-1}$. By Lemma 3.42, the erea of $(k(B),k(0),0)$ is therefore

$$\begin{aligned} \frac{1-\overline{k(B)}k(0)}{1-k(B)\overline{k(0)}} &= \left(\frac{A\overline{B}-1-A\overline{B}+A\overline{A}}{A\overline{B}-1}\right)\left(\frac{\overline{A}B-1}{\overline{A}B-1-\overline{A}B+A\overline{A}}\right) \\ &= \frac{\overline{A}B-1}{A\overline{B}-1} = \frac{1-\overline{A}B}{1-A\overline{B}}. \quad \square \end{aligned}$$

I.e., the element $k(z) = \dfrac{z-A}{\overline{A}z-1} \in U$ preserves the erea of $(A,B,0)$.

Definition: The **erea** of (P,Q,R) is the erea of $(g(P),g(Q),0)$ where $g \in U, g(R) = 0$.

Lemma 3.44. *The erea of (P, Q, R) is well-defined.*

Proof: Since $(P,Q,R) = (Q,R,P)$, the definition of erea depends on both the vertex sent to 0 and the element of U sending it to 0. Let $V, W \in \{P,Q,R\}$. Let $g, h \in U$ such that $g(V) = 0, h(W) = 0$. If $V = W$, then $g \circ h^{-1}(0) = 0$ and so $g \circ h^{-1} \in \mathbb{S}z \leq B$. Since B preserves ratios, it preserves erea. Thus, h and $g = t \circ h,\ t \in B$ give the same erea.

If $V \neq W$, let $k(z) = \dfrac{z - g(W)}{\overline{g(W)}z - 1}$. Then $k \circ g \circ h^{-1} \in B$ and $h = t \circ k \circ g$ where $t \in B$. Thus, h and g give the same erea by Lemma 3.43. $\square$

Notation: In (A,B,C), let $\alpha = \text{den}(\ M(C,A),\ M(A,B),\ A\ )$, $\beta = \text{den}(\ M(A,B),\ M(B,C),\ B\ )$, $\gamma = \text{den}(M(B,C),\ M(C,A),\ C\ )$ and δ be the erea of (A,B,C). Also let $a = \triangle(B,C)$, $b = \triangle(A,C)$ and $c = \triangle(A,B)$.

We define $\cosh(c) = 1 + 2\triangle(A,B)$.

Theorem 3.45. *(First Cosh Law)*

In (A,B,C),

$$\cosh(c) \ = \ \cot(\alpha)\cot(\beta) \ + \ \frac{\cos\gamma}{\sin(\alpha)\sin(\beta)}.$$

Proof: Now

$$\cot(\alpha)\cot(\beta) \ + \ \frac{\cos\gamma}{\sin(\alpha)\sin(\beta)} \ = \ \frac{-(\alpha+1)(\beta+1)}{(\alpha-1)(\beta-1)} \ + \ \frac{2(\gamma+1)\alpha\beta\delta}{(\alpha-1)(\beta-1)}.$$

We may assume $C = 0$. Let D be the Euclidean center of $M(A,B)$. We know $0 \neq |D-A|^2 = |D-B|^2 = D\overline{D} - 1,\ A\overline{A} \neq 1 \neq B\overline{B},\ A\overline{B} \neq 1$. Also

$$\alpha \ = \ \frac{-\overline{A}(D-A)}{A(\overline{D-A})}, \ \beta \ = \ \frac{-B(\overline{D-B})}{\overline{B}(D-B)}, \ \gamma \ = \ \frac{A\overline{B}}{\overline{A}B}.$$

From Lemma 3.42 and its proof,

$$\delta = \frac{1-\overline{A}B}{1-A\overline{B}}, \quad D-B = \frac{(A-B)(1-\overline{A}B)}{A\overline{B}-\overline{A}B}, \quad D-A = \frac{(A-B)(1-A\overline{B})}{A\overline{B}-\overline{A}B}.$$

Thus,

$$\alpha = \frac{\overline{A}(A-B)(1-A\overline{B})}{A(\overline{A-B})(1-\overline{A}B)}, \quad \beta = \frac{B(\overline{A-B})(1-A\overline{B})}{\overline{B}(A-B)(1-\overline{A}B)}, \quad \gamma+1 = \frac{A\overline{B}+\overline{A}B}{\overline{A}B},$$

$$\alpha-1 = \frac{(A\overline{B}-\overline{A}B)(1-A\overline{A})}{A(\overline{A-B})(1-\overline{A}B)}, \quad \alpha+1 = \frac{2A\overline{A}(1+B\overline{B})-(A\overline{B}+\overline{A}B)(1+A\overline{A})}{A(\overline{A-B})(1-\overline{A}B)},$$

$$\beta-1 = \frac{\overline{A}B-A\overline{B})(1-B\overline{B})}{\overline{B}(A-B)(1-\overline{A}B)}, \quad \beta+1 = \frac{-2B\overline{B}(1+A\overline{A})+(\overline{A}B+A\overline{B})(1+B\overline{B})}{\overline{B}(A-B)(1-\overline{A}B)}.$$

Now

$$\begin{aligned} 1+2\Delta(A,B) &= \frac{(1-A\overline{A})(1-B\overline{B})+2(A-B)(\overline{A-B})}{(1-A\overline{A})(1-B\overline{B})} \\ &= \frac{1+A\overline{A}+B\overline{B}+A\overline{A}B\overline{B}-2\overline{A}B-2A\overline{B}}{(1-A\overline{A})(1-B\overline{B})}. \end{aligned}$$

Note that

$$[2A\overline{A}(1+B\overline{B})-(A\overline{B}+\overline{A}B)(1+A\overline{A})][-2B\overline{B}(1+A\overline{A})+(\overline{A}B+A\overline{B})(1+B\overline{B})]$$

$$\begin{aligned} &= -4A\overline{A}B\overline{B}(1+A\overline{A})(1+B\overline{B})+2B\overline{B}(1+A\overline{A})(1+A\overline{A})(A\overline{B}+\overline{A}B) \\ &+ 2A\overline{A}(1+B\overline{B})(1+B\overline{B})(\overline{A}B+A\overline{B}) \\ &- 2(A\overline{B}+\overline{A}B)(\overline{A}B+A\overline{B})(1+A\overline{A})(1+B\overline{B}) \end{aligned}$$

$$\begin{aligned} = \ & [\,-4A\overline{A}B\overline{B}-4A^2\overline{A}^2B\overline{B}-4A\overline{A}B^2\overline{B}^2-4A^2\overline{A}^2B^2\overline{B}^2\,] \\ &+ [\,2AB\overline{B}^2+4A^2\overline{A}B\overline{B}^2+2A^3\overline{A}^2B\overline{B}^2+2\overline{A}B^2\overline{B}+4A\overline{A}^2B^2\overline{B}+2A^2\overline{A}^3B^2\overline{B}\,] \\ &+ [\,2A\overline{A}^2B+4A\overline{A}^2B^2\overline{B}+2A\overline{A}^2B^3\overline{B}^2+2A^2\overline{AB}+4A^2\overline{A}B\overline{B}^2+2A^2\overline{A}B^2\overline{B}^3\,] \\ &+ [\,-2A\overline{A}B\overline{B}-\overline{A}^2B^2-A^2\overline{B}^2-2A^2\overline{A}^2B\overline{B}-A\overline{A}^3B^2-A^3\overline{A}(\overline{B})^2 \\ &- 2A\overline{A}B^2\overline{B}^2-\overline{A}^2B^3\overline{B}-A^2B\overline{B}^3-2A^2\overline{A}^2B^2\overline{B}^2-A\overline{A}^3B^3\overline{B}-A^3\overline{A}B\overline{B}^3]. \end{aligned}$$

So

$$
\begin{aligned}
P := & -[\, 2A\overline{A}(1+B\overline{B}) - (A\overline{B}+\overline{A}B)(1+A\overline{A}) \,] \\
& \qquad\qquad [\, -2B\overline{B}(1+A\overline{A}) + (\overline{A}B + A\overline{B})(1+B\overline{B}) \,] \\
= & \;\; 6A\overline{A}B\overline{B} + 6A\overline{A}B^2\overline{B}^2 - 8A\overline{A}^2B^2\overline{B} - 2A\overline{A}^2B^3\overline{B}^2 + A\overline{A}^3B^3\overline{B} + 6A^2\overline{A}^2B\overline{B} \\
& + \; 6A^2\overline{A}^2B^2\overline{B}^2 - 8A^2\overline{A}B\overline{B}^2 - 2A^2\overline{A}^3B^2\overline{B} - 2A^2\overline{A}B^2\overline{B}^3 - 2A^2\overline{A}B\overline{B}^3 \\
& - \; 2A^3\overline{A}^2B\overline{B}^2 + A^3\overline{A}B\overline{B}^2 + A^3\overline{A}B\overline{B}^3 - 2AB\overline{B}^2 - 2\overline{A}B^2\overline{B} - 2A\overline{A}^2B \\
& - \; 2A^2\overline{AB} + A\overline{A}^3B^2 + \overline{A}^2B^3\overline{B} - 2A^2\overline{AB} + A^2B\overline{B}^3 + \overline{A}^2B^2 + A^2\overline{B}^2.
\end{aligned}
$$

Thus,

$$
\begin{aligned}
& -(\alpha+1)(\beta+1) \\
&= -\left[\frac{2A\overline{A}(1+B\overline{B}) - (A\overline{B}+\overline{A}B)(1+A\overline{A})}{A(\overline{A}-\overline{B})(1-\overline{A}B)}\right]\left[\frac{-2B\overline{B}(1+A\overline{A}) + (\overline{A}B+A\overline{B})(1+B\overline{B})}{\overline{B}(A-B)(1-\overline{A}B)}\right] \\
&= \frac{P}{A\overline{B}(A-B)(\overline{A}-\overline{B})(1-\overline{A}B)^2}
\end{aligned}
$$

Now

$$
\begin{aligned}
2(\gamma+1)\alpha\beta\delta &= \frac{2(A\overline{B}+\overline{A}B)(1-A\overline{B})}{A\overline{B}(1-\overline{A}B)} \\
&= \frac{2(A\overline{B}+\overline{A}B)(1-A\overline{B})(1-\overline{A}B)(A-B)(\overline{A}-\overline{B})}{A\overline{B}(A-B)(\overline{A}-\overline{B})(1-\overline{A}B)^2} \\
&= \frac{(2A\overline{B}+2\overline{A}B)[\,(1-A\overline{B}-\overline{A}B+A\overline{A}B\overline{B})(A\overline{A}+B\overline{B}-\overline{A}B-A\overline{B})\,]}{A\overline{B}(A-B)(\overline{A}-\overline{B})(1-\overline{A}B)^2} \\
&= \frac{Q}{A\overline{B}(A-B)(\overline{A}-\overline{B})(1-\overline{A}B)^2}
\end{aligned}
$$

where

$$
\begin{aligned}
Q \; := & \;\; (2A\overline{B}+2\overline{A}B)[\, A\overline{A} + B\overline{B} - \overline{A}B - A\overline{B} - A^2\overline{AB} - AB\overline{B}^2 + 2A\overline{A}B\overline{B} + A^2\overline{B}^2 \\
& - \; A\overline{A}^2B - \overline{A}B^2\overline{B} + \overline{A}^2B^2 + 2\overline{A}B + A^2\overline{A}^2B\overline{B} + A\overline{A}B^2\overline{B}^2 \\
& - \; A\overline{A}^2B^2\overline{B} - A^2\overline{A}B\overline{B}^2 \,]
\end{aligned}
$$

$$
\begin{aligned}
= & \ [\, 2\overline{A}^3 B^3 + 2A^3\overline{B}^3 - 2A^2\overline{B}^2 - 2\overline{A}^2 B^2 + 2A^2\overline{AB} + 2A\overline{A}^2 B + 2AB\overline{B}^2 + 2\overline{A}B^2\overline{B} \\
- & \ 2A^3\overline{A}(\overline{B})^2 - 2A^2 B\overline{B}^3 - 2A\overline{A}^3 B^2 - 2\overline{A}^2 B^3\overline{B} - 4A\overline{A}B\overline{B} + 2A^3\overline{A}^2 B\overline{B}^2 \\
+ & \ 2A^3\overline{A}B\overline{B}^3 - 4A^2\overline{A}^2 B\overline{B} + 6A^2\overline{A}B\overline{B}^2 + 2A^2\overline{A}B^2\overline{B}^3 - 4A^2\overline{A}^2 B^2\overline{B}^2 \\
+ & \ 2A^2\overline{A}^3 B^2\overline{B} - 4A\overline{A}B^2\overline{B}^2 - 2A\overline{A}^3 B^3\overline{B} + 2A\overline{A}^2 B^3\overline{B}^2 + 6A\overline{A}^2 B^2\overline{B}\,].
\end{aligned}
$$

Then

$$
-(\alpha+1)(\beta+1) + 2(\gamma+1)\alpha\beta\delta = \frac{X}{A\overline{B}(A-B)(\overline{A-B})(1-\overline{A}B)^2}
$$

where

$$
\begin{aligned}
X &= P(1-\overline{A}B) + Q \\
&= 2A\overline{A}B\overline{B} + 2A\overline{A}B^2\overline{B}^2 - 2A\overline{A}^2 B^2\overline{B} - A\overline{A}^3 B^3\overline{B} + 2A^2\overline{A}^2 B\overline{B} + 2A^2\overline{A}^2 B^2\overline{B}^2 \\
&\quad - 2A^2\overline{A}B\overline{B}^2 - A^3\overline{A}(\overline{B})^2 - A^3\overline{A}B\overline{B}^3 - A\overline{A}^3 B^2 - \overline{A}^2 B^3\overline{B} - A^2 B\overline{B}^3 + 2\overline{A}^3 B^3 \\
&\quad + 2A^3\overline{B}^3 - A^2\overline{B}^2 - \overline{A}^2 B^2.
\end{aligned}
$$

Now

$$
(\alpha-1)(\beta-1) = \frac{(A\overline{B}-\overline{A}B)(1-A\overline{A})(\overline{A}B-A\overline{B})(1-B\overline{B})}{A(\overline{A-B})(1-\overline{A}B)\overline{B}(A-B)(1-\overline{A}B)}.
$$

Thus,

$$
\frac{-(\alpha+1)(\beta+1)+2(\gamma+1)(\alpha\beta\delta)}{(\alpha-1)(\beta-1)} = \frac{X}{(1-A\overline{A})(1-B\overline{B})(A\overline{B}-\overline{A}B)(\overline{A}B-A\overline{B})}.
$$

But

$$
\begin{aligned}
X = &\ 2A\overline{A}B\overline{B} - \overline{A}^2 B^2 - A^2\overline{B}^2 + 2A^2\overline{A}^2 B\overline{B} - A\overline{A}^3 B^2 - A^3\overline{A}(\overline{B})^2 \\
&+ 2A\overline{A}B^2\overline{B}^2 - \overline{A}^2 B^3\overline{B} - A^2 B\overline{B}^3 + 2A^2\overline{A}^2 B^2\overline{B}^2 - A\overline{A}^3 B^3\overline{B} - A^3\overline{A}B\overline{B}^3 \\
&- 2A\overline{A}^2 B^2\overline{B} + 2\overline{A}^3 B^3 - 2A^2\overline{A}B\overline{B}^2 + 2A^3\overline{B}^3 \\
= &\ (\, 1 + A\overline{A} + B\overline{B} + A\overline{A}B\overline{B} - 2\overline{A}B - 2A\overline{B}\,)(\, 2A\overline{A}B\overline{B} - \overline{A}^2 B^2 - A^2\overline{B}^2\,) \\
= &\ (\, 1 + A\overline{A} + B\overline{B} + A\overline{A}B\overline{B} - 2\overline{A}B - 2A\overline{B}\,)(\, A\overline{B} - \overline{A}B\,)(\, \overline{A}B - A\overline{B}\,).
\end{aligned}
$$

Thus,

$$\frac{1 + A\overline{A} + B\overline{B} + A\overline{A}B\overline{B} - 2\overline{A}B - 2A\overline{B}}{(1 - A\overline{A})(1 - B\overline{B})}$$
$$= \frac{X}{(1 - A\overline{A})(1 - B\overline{B})(A\overline{B} - \overline{A}B)(\overline{A}B - A\overline{B})}. \quad \square$$

Note that $(\alpha + 1)^2(\beta + 1)^2 - (\alpha - 1)^2(\beta - 1)^2 = 4(\alpha + \beta)(1 + \alpha\beta)$ and $\alpha^2\beta^2\delta = \alpha^2\beta^2\left(\frac{1}{\alpha\beta\delta}\right) = \frac{\alpha\beta}{\gamma}$.

Thus,

$$\begin{aligned}
(\sinh c)^2 &= (\cosh c)^2 - 1 \\
&= \left[\frac{-(\alpha+1)(\beta+1) + 2(\gamma+1)\alpha\beta\delta}{(\alpha-1)(\beta-1)}\right]^2 - 1 \\
&= \frac{(\alpha+1)^2(\beta+1)^2 - (\alpha-1)^2(\beta-1)^2 - 4(\alpha+1)(\beta+1)(\gamma+1)\alpha\beta\delta + 4(\gamma+1)^2\alpha^2\beta^2\delta}{(\alpha-1)^2(\beta-1)^2} \\
&= \frac{4\left[(\alpha+B)(1+\alpha\beta) - (\alpha+1)(\beta+1)(\gamma+1)\alpha\beta\delta + (\gamma+1)^2\frac{\alpha\beta}{\gamma}\right]}{(\alpha-1)^2(\beta-1)^2}.
\end{aligned}$$

We therefore have the following hyperbolic trig formulas.

i) $\cosh c = \dfrac{-(\alpha+1)(\beta+1) + 2(\gamma+1)\alpha\beta\delta}{(\alpha-1)(\beta-1)}$

ii)

$$(\sinh c)^2 = \frac{4\left[(\alpha+\beta)(1+\alpha\beta) + (\gamma+1)^2\left(\frac{\alpha\beta}{\gamma}\right) - (\alpha+1)(\beta+1)(\gamma+1)\alpha\beta\delta\right]}{(\alpha-1)^2(\beta-1)^2}$$

The analogous formulas hold for sides a and b.

In the classical case, a hyperbolic triangle is determined (up to isometery) by its dengles.

Notation: In (A, B, C), let $\alpha_1 = \text{den}(\ M(C,A),\ M(A,B),\ A\ )$, $\beta_1 = \text{den}(M(A,B), M(B,C), B)$, $\gamma_1 = \text{den}(M(B,C),\ M(C,A),\ C\ )$ and δ_1 be the erea of (A,B,C). In (P,Q,R), let $\alpha_2 = \text{den}(\ M(R,P),\ M(P,Q),\ P\ )$, $\beta_2 = \text{den}(M(P,Q), M(Q,R), Q)$, $\gamma_2 = \text{den}(M(Q,R),\ M(R,P),\ R\ )$ and δ_2 be the erea of (P,Q,R).

If $\alpha_1 = \alpha_2$, $\beta_1 = \beta_2$ and $\gamma_1 = \gamma_2$, then

$$(\delta_1)^2 = \frac{1}{\alpha_1\beta_1\gamma_1} = \frac{1}{\alpha_2\beta_2\gamma_2} = (\delta_2)^2.$$

Thus, $\delta_1 = \pm\,\delta_2$.

Theorem 3.46. *If all the corresponding dengles of (A,B,C) and (P,Q,R) are equal, they are isometric if and only if their ereas are equal.*

Proof: If $\delta_1 = \delta_2$, then

$$1 + 2\triangle(A,B) = \frac{-(\alpha_1+1)(\beta_1+1)}{(\alpha_1-1)(\beta_1-1)} + \frac{2(\gamma_1+1)\alpha_1\beta_1\delta_1}{(\alpha_1-1)(\beta_1-1)} = 1 + 2\triangle(P,Q)$$

by the First Cosh Law. Similarly, $\triangle(B,C) = \triangle(Q,R)$ and $\triangle(A,C) = \triangle(P,R)$. Consequently, the two triangles are isometric by SSS.

Conversely, if the triangles are isometric then $\delta_1 = \delta_2$ since isometries preserve erea. □

If at least one of α_1, β_1, γ_1 is a right dengle, then (A,B,C) and (P,Q,R) are weakly isometric (but not necessarily isometric). For we may assume $\gamma_1 = -1$. Then by the First Cosh Law,

$$1 + 2\triangle(A,B) = \frac{-(\alpha_1+1)(\beta_1+1)}{(\alpha_1-1)(\beta_1-1)} = 1 + 2\triangle(P,Q).$$

Thus, $\triangle(A,B) = \triangle(P,Q)$ and $(A,B,C) \cong_W (P,Q,R)$ by DSD.

One can still hope that if none of the dengles of (A, B, C) are right dengles, then the derea is determined by the dengles. We now investigate this possibility.

Continuing with the notation above Theorem 3.46, we may assume $C = 0 = R$. Suppose that $\gamma_1 = \gamma_2$. Then $\gamma_1 = \dfrac{A\overline{B}}{\overline{A}B} = \dfrac{P\overline{Q}}{\overline{P}Q} = \gamma_2$ by (the proof of) Lemma 3.42. Consequently, $\rho(Q) = \dfrac{Q}{\overline{Q}} = \dfrac{\overline{A}BP}{A\overline{B}\overline{P}} = \rho(\dfrac{BP}{A})$. Since $\ker(\rho) = \mathbb{F}^{\times}$, $Q = \dfrac{\lambda PB}{A}$ for some $\lambda \in \mathbb{F}^{\times}$.

Conversely, given a triangle (A, B, O), for any $O \neq P \in \mathbb{D}$, $(P, \frac{BP}{A}, O)$ is a triangle with $\gamma_1 = \gamma_2$.

The question thus becomes

Given (A, B, O), when can we choose a $P \in \mathbb{D}$ so that $\alpha_1 = \alpha_2$ in (A, B, O) and $(P, \frac{\lambda BP}{A}, O)$ but $\delta_1 = -\delta_2$?

We recall from Lemma 3.42 and its proof, that the erea of $\triangle(A, B, O)$ is $\dfrac{1-\overline{A}B}{1-A\overline{B}}$ and the erea of $\triangle(P, Q, O)$ is $\dfrac{1-\overline{P}Q}{1-P\overline{Q}}$. Also

$$\begin{aligned}
\alpha_1 &= \frac{\overline{A}(A-B)(1-A\overline{B})}{A(\overline{A}-\overline{B})(1-\overline{A}B)}, \quad \alpha_2 = \frac{\overline{P}(P-Q)(1-P\overline{Q})}{P(\overline{P}-\overline{Q})(1-\overline{P}Q)},\\
\beta_1 &= \frac{B(\overline{A}-\overline{B})(1-A\overline{B})}{\overline{B}(A-B)(1-\overline{A}B)}, \quad \beta_2 = \frac{Q(\overline{P}-\overline{Q})(1-P\overline{Q})}{\overline{Q}(P-Q)(1-\overline{P}Q)},\\
\gamma_1 &= \frac{A\overline{B}}{\overline{A}B}, \quad \gamma_2 = \frac{P\overline{Q}}{\overline{P}Q}.
\end{aligned}$$

Claim 1. $\alpha_2 = \left[\dfrac{\overline{A}(A-\lambda B)}{A(\overline{A}-\lambda\overline{B})}\right]\left[\dfrac{1}{\delta_2}\right]$.

Proof: In $(P, Q = \frac{\lambda BP}{A}, O)$,

$$\alpha_2 = \frac{\overline{P}(P-Q)(1-P\overline{Q})}{P(\overline{P}-\overline{Q})(1-\overline{P}Q)} = \frac{\overline{P}(P-Q)}{P(\overline{P}-\overline{Q})}\left(\frac{1}{\delta_2}\right).$$

But

$$\frac{\overline{P}(P-Q)}{P(\overline{P}-\overline{Q})} = \frac{\overline{P}\left(P-\dfrac{\lambda BP}{A}\right)}{P\left(\overline{P}-\dfrac{\lambda\overline{B}\overline{P}}{\overline{A}}\right)} = \frac{1-\dfrac{\lambda B}{A}}{1-\dfrac{\lambda\overline{B}}{\overline{A}}} = \frac{\overline{A}(A-\lambda B)}{A(\overline{A}-\lambda\overline{B})}. \quad \square$$

Claim 2. *$-\left(\dfrac{A-\lambda B}{\overline{A}-\lambda\overline{B}}\right) = \dfrac{A-B}{\overline{A}-\overline{B}}$ if and only if $Re(A\overline{B}) = A\overline{A} = B\overline{B}$ or $\lambda = \dfrac{-(2A\overline{A}-A\overline{B}-\overline{A}B)}{2B\overline{B}-A\overline{B}-\overline{A}B}$.*

Proof: $-\left(\dfrac{A-\lambda B}{\overline{A}-\lambda\overline{B}}\right) = \dfrac{A-B}{\overline{A}-\overline{B}}$

$$\iff -A\overline{A}+\lambda\overline{A}B+A\overline{B}-\lambda B\overline{B} = A\overline{A}-\lambda A\overline{B}-\overline{A}B+\lambda B\overline{B}$$

$$\iff -2A\overline{A}+A\overline{B}+\overline{A}B = \lambda(2B\overline{B}-A\overline{B}-\overline{A}B)$$

$$\iff \lambda(2B\overline{B}-A\overline{B}-\overline{A}B) = -(2A\overline{A}-A\overline{B}-\overline{A}B)$$

$$\iff \lambda = \frac{-(2A\overline{A}-A\overline{B}-\overline{A}B)}{2B\overline{B}-A\overline{B}-\overline{A}B} \quad \text{or} \quad 2A\overline{A}=2B\overline{B}=A\overline{B}+\overline{A}B. \quad \square$$

Claim 3. *If $O \neq P \in \mathbb{D}$, $\lambda \in \mathbb{F}^{\times}$ and $Q = \dfrac{\lambda BP}{A}$, then $\dfrac{1-\overline{P}Q}{1-P\overline{Q}} = -\left(\dfrac{1-\overline{A}B}{1-A\overline{B}}\right)$ if and only if $Re(A\overline{B}) = A\overline{A}B\overline{B}=1$ or*

$$P\overline{P} = \frac{A\overline{A}}{\lambda}\left[\frac{(1-\overline{A}B)+(1-A\overline{B})}{A\overline{B}(1-\overline{A}B)+\overline{A}B(1-A\overline{B})}\right] = \frac{-A\overline{A}}{\lambda}\left[\frac{2-A\overline{B}-\overline{A}B}{2A\overline{A}B\overline{B}-A\overline{B}-\overline{A}B}\right].$$

Proof: $\dfrac{1-\overline{P}Q}{1-P\overline{Q}} = \dfrac{1-\dfrac{\lambda BP\overline{P}}{A}}{1-\dfrac{\lambda\overline{B}P\overline{P}}{\overline{A}}} = \dfrac{\overline{A}(A-\lambda BP\overline{P})}{A(\overline{A}-\lambda\overline{B}P\overline{P})}$. Therefore,

$$\frac{1-\overline{A}B}{1-A\overline{B}} = \frac{-\overline{A}(A-\lambda BP\overline{P})}{A(\overline{A}-\lambda\overline{B}P\overline{P})}$$

$$\iff A(\overline{A}-\overline{A}^2B-\lambda\overline{B}P\overline{P}+\lambda\overline{A}B\overline{B}P\overline{P}) = -\overline{A}(A-A^2\overline{B}-\lambda BP\overline{P}+\lambda AB\overline{B}P\overline{P})$$

$$\iff \lambda P\overline{P}(2A\overline{A}B\overline{B}-A\overline{B}-\overline{A}B) = -A\overline{A}(2-A\overline{B}-\overline{A}B)$$

$$\iff P\overline{P} = \frac{-A\overline{A}(2-A\overline{B}-\overline{A}B)}{\lambda(2A\overline{A}B\overline{B}-A\overline{B}-\overline{A}B)} \quad \text{or} \quad 2A\overline{A}B\overline{B} = A\overline{B}+\overline{A}B = 2. \quad \square$$

Claims 1, 2 and 3 give the following theorem.

Theorem 3.47. *Let (A,B,O) be a triangle in $\mathbb{D}$ such that Re($A\overline{B}$) $\notin \{ B\overline{B}, A\overline{A}B\overline{B} \}$.*

Assume $O \neq P \in \mathbb{D}$, $\lambda \in \mathbb{F}^{\times}$ and $Q = \dfrac{\lambda BP}{A}$. Then $\alpha_1 = \alpha_2$ and $\delta_1 = -\delta_2$ if and only if $\lambda = \dfrac{-(2A\overline{A} - A\overline{B} - \overline{A}B)}{2B\overline{B} - A\overline{B} - \overline{A}B}$ and $P\overline{P} = \dfrac{-A\overline{A}}{\lambda}\left[\dfrac{2 - A\overline{B} - \overline{A}B}{2A\overline{A}B\overline{B} - A\overline{B} - \overline{A}B}\right]$.

Theorem 3.48. *Let (A,B,O) be a triangle in $\mathbb{D}$ such that Re($A\overline{B}$) $= B\overline{B} = A\overline{A}$ or Re($A\overline{B}$) $= A\overline{A}B\overline{B} = 1$. Then there is a triangle with the same dengle data as (A,B,O) but with a different erea.*

Proof: Case 1: $\mathrm{Re}(A\overline{B}) = B\overline{B} = A\overline{A}$

In other words, $2A\overline{A} = 2B\overline{B} = A\overline{B} + \overline{A}B$. Then $-\left(\dfrac{A-\lambda B}{\overline{A}-\lambda\overline{B}}\right) = \dfrac{A-B}{\overline{A}-\overline{B}}$ by Claim 2. If $2A\overline{A}B\overline{B} = A\overline{B}+\overline{A}B = 2$, then the erea of $(P, \frac{\lambda BP}{A}, O)$ and (A,B,O) are negatives by Claim 3 for any choices of $O \neq P \in \mathbb{D}$ and $\lambda \in \mathbb{F}^{\times}$. Otherwise, we can choose any $\lambda \in \mathbb{F}^{\times}$ and any $P \in \mathbb{D}$ with $P\overline{P} = \dfrac{-A\overline{A}(2-2A\overline{A})}{\lambda(2(A\overline{A})^2 - 2A\overline{A})} = \dfrac{1}{\lambda}$. Such a choice will work by Claim 3. In either case, we have $\alpha_1 = \alpha_2$ by Claim 1. □

Case 2: $\mathrm{Re}(A\overline{B}) = A\overline{A}B\overline{B} = 1$.

Then $2A\overline{A}B\overline{B} = A\overline{B} + \overline{A}B = 2$. By Claim 3, $\delta_1 = \delta_2$ for any $O \neq P \in \mathbb{D}$ and $\lambda \in \mathbb{F}^{\times}$. If $2A\overline{A} = 2B\overline{B} = A\overline{B} + \overline{A}B$, then $\alpha_1 = \alpha_2$ by Claims 1 and 2. Otherwise, if

$$\lambda = -\left[\frac{2A\overline{A} - (A\overline{B} + \overline{A}B)}{2B\overline{B} - (A\overline{B} + \overline{A}B)}\right] = -\left[\frac{2A\overline{A} - 2}{2B\overline{B} - 2}\right] = \frac{1 - A\overline{A}}{B\overline{B} - 1},$$

then $\alpha_1 = \alpha_2$ again by Claims 1 and 2. □

Claim 4. *Assume (A,B,O) is a triangle in $\mathbb{D}$. Assume $Q = \dfrac{\lambda BP}{A}$,*
$P\overline{P} = \dfrac{-A\overline{A}}{\lambda}\left[\dfrac{2-A\overline{B}-\overline{A}B}{2A\overline{A}B\overline{B}-A\overline{B}-\overline{A}B}\right]$, *and* $\lambda = \dfrac{-(2A\overline{A}-A\overline{B}-\overline{A}B)}{2B\overline{B}-A\overline{B}-\overline{A}B} \neq 0$.
Then $P\overline{P} \neq 1$.

Proof: Let $X = A\overline{B}+\overline{A}B$. Since $\lambda \neq 0$,

$$P\overline{P} = A\overline{A}\left[\frac{2-X}{2A\overline{A}B\overline{B}-X}\right]\left[\frac{2B\overline{B}-X}{2A\overline{A}-X}\right].$$

If $P\overline{P} = 1$, then

$$A\overline{A}(2-X)(2B\overline{B}-X) = (2A\overline{A}B\overline{B}-X)(2A\overline{A}-X)$$

$$\Longrightarrow A\overline{A}(4B\overline{B}-2B\overline{B}X-2X+X^2) = 4(A\overline{A})^2B\overline{B}-2A\overline{A}X-2A\overline{A}B\overline{B}X+X^2$$

$$\Longrightarrow 4A\overline{A}B\overline{B}+A\overline{A}X^2-4(A\overline{A})^2B\overline{B}-X^2 = 0$$

$$\Longrightarrow (1-A\overline{A})(4A\overline{A}B\overline{B}-X^2) = 0 \Longrightarrow 4A\overline{A}B\overline{B} = X^2 = (A\overline{B}+\overline{A}B)^2$$

$$\Longrightarrow (A\overline{B}-\overline{A}B)^2 = 0 \Longrightarrow A\overline{B} = \overline{A}B \Longrightarrow \gamma_1 = 1.$$

This is a contradiction and therefore $P\overline{P} \neq 1$. □

We have now established the following theorem.

Theorem 3.49. *Let (A,B,O) be a triangle in $\mathbb{D}$. Then there exists a $0 \neq P \in \mathbb{D}$ and $\lambda \in \mathbb{F}^{\times}$ such that $(P, Q = \dfrac{\lambda BP}{A}, O)$ and (A,B,O) have the same dengle data but different ereas if and only if neither of the following occur: $Re(A\overline{B}) \in \{A\overline{A}, B\overline{B}\}$ but $A\overline{A} \neq B\overline{B}$ or $Re(A\overline{B}) \in \{A\overline{A}B\overline{B}, 1\}$ but $A\overline{A}B\overline{B} \neq 1$. Moreover, unless $Re(A\overline{B}) = A\overline{A} = B\overline{B}$ or $Re(A\overline{B}) = 1 = A\overline{A}B\overline{B}$, $P\overline{P}$ and λ are uniquely given by the formulas*

$$\lambda = \frac{-(2A\overline{A}-A\overline{B}-\overline{A}B)}{2B\overline{B}-A\overline{B}-\overline{A}B}, \quad P\overline{P} = \frac{-A\overline{A}}{\lambda}\left[\frac{2-A\overline{B}-\overline{A}B}{2A\overline{A}B\overline{B}-A\overline{B}-\overline{A}B}\right].$$

If $\mathbb{F} = \mathbb{F}_5$ and $\mathbb{E} = \mathbb{F}_{25}$, there are no examples of two triangles with the same dengle data but different ereas unless at least one of the dengles is -1. Write $\mathbb{E} = \mathbb{F} \oplus \mathbb{F}\alpha$ where α is a root of $x^2 + 2$ in $\mathbb{E}$. Let $A = 2, B = \alpha$. Using the equations from Theorem 3.49 we get $\lambda = -2, P\overline{P} = -1$. If we choose $P = -1 + 2\alpha$, then $Q = -1 + \alpha$ and (A, B, O) and (P, Q, O) are triangles with different ereas $(\pm(2 - \alpha))$ but the same dengle data (dengles $2 - \alpha, -1, -1$).

Let $\mathbb{F} = \mathbb{F}_{11}, \mathbb{E} = \mathbb{F}_{121}$ and write $\mathbb{E} = \mathbb{F} \oplus \mathbb{F}i$ where i is a root of $x^2 + 1$ in $\mathbb{E}$. Let $A = 4, B = 1 + 2i, P = 2, Q = 5 - i$. Then (A, B, O) and (P, Q, O) have different ereas $(\pm i)$ but the same dengle data (all dengles equal to $-5 - 3i$).

Theorem 3.50. *(Hyperbolic Pythagorean Theorem)*

If $\gamma = -1$ *in* (A, B, C), *then* $\cosh(c) = \cosh(a)\cosh(b)$.

Proof: Since $\gamma = -1$,

$$\begin{aligned}
\cosh c &= \frac{-(\alpha+1)(\beta+1)}{(\alpha-1)(\beta-1)}, \quad \cosh a = \frac{2(\alpha+1)\beta\gamma\delta}{(\beta-1)(\gamma-1)} = \frac{-(\alpha+1)\beta\delta}{(\beta-1)} \\
\cosh b &= \frac{2(\beta+1)\alpha\gamma\delta}{(\alpha-1)(\gamma-1)} = \frac{-(\beta+1)\alpha\delta}{\alpha-1}.
\end{aligned}$$

Thus,

$$\cosh(a)\cosh(b) = \frac{\alpha\beta\delta^2(\alpha+1)(\beta+1)}{(\alpha-1)(\beta-1)} = \frac{-(\alpha+1)(\beta+1)}{(\alpha-1)(\beta-1)}. \quad \square$$

Remark:

$$\begin{aligned}
\cosh(c) &= \cosh(a)\cosh(b) \\
&\iff 1 + 2\Delta(A, B) = (\ 1 + 2\Delta(B, C)\ )(\ 1 + 2\Delta(A, C)\ ) \\
&\iff 1 + 2\Delta(A, B) = 1 + 2\Delta(B, C) + 2\Delta(A, C) + 4\Delta(B, C)\Delta(A, C) \\
&\iff \Delta(A, B) = \Delta(B, C) + \Delta(A, C) + 2\Delta(B, C)\Delta(A, C).
\end{aligned}$$

Thus, the Hyperbolic Pythagorean Theorem says

$$\gamma = -1 \iff \Delta(A,B) = \Delta(B,C) + \Delta(A,C) + 2\Delta(B,C)\Delta(A,C).$$

Theorem 3.51. *(Sinh Law) In* (A, B, C)*,*

$$\frac{\sinh^2(a)}{\sinh^2(\alpha)} = \frac{\sinh^2(b)}{\sinh^2(\beta)} = \frac{\sinh^2(c)}{\sinh^2(\gamma)}.$$

Proof: First note that $\sin^2(\theta) = \dfrac{(\theta-1)^2}{-4\theta} \neq 0$ for $\theta \in \{\ \alpha, \beta, \gamma\ \}$ and $\sinh^2(x) = [\,2\Delta(y,z)+1\,]^2 - 1 \neq 0$ for $x, y, z \in \{\ a, b, c\ \}$. Thus, it is equivalent to prove

$$\frac{\sinh^2(a)}{\sinh^2(c)} = \frac{\sinh^2(\alpha)}{\sinh^2(\gamma)} \quad \text{and} \quad \frac{\sinh^2(b)}{\sinh^2(c)} = \frac{\sinh^2(\beta)}{\sinh^2(\gamma)}.$$

Let

$$\begin{aligned}
X &= (\beta+\gamma)(1+\beta\gamma) + (\alpha+1)^2\left(\frac{\beta\gamma}{\alpha}\right) - (\alpha+1)(\beta+1)(\gamma+1)\beta\gamma\delta,\\
Y &= (\alpha+\gamma)(1+\alpha\gamma) + (\beta+1)^2\left(\frac{\alpha\gamma}{\beta}\right) - (\alpha+1)(\beta+1)(\gamma+1)\alpha\gamma\delta,\\
Z &= (\alpha+\beta)(1+\alpha\beta) + (\gamma+1)^2\left(\frac{\alpha\beta}{\gamma}\right) - (\alpha+1)(\beta+1)(\gamma+1)\alpha\beta\delta.
\end{aligned}$$

Then

$$\begin{aligned}
(\sinh a)^2 &= \frac{4X}{(\beta-1)^2(\gamma-1)^2},\\
(\sinh b)^2 &= \frac{4Y}{(\alpha-1)^2(\gamma-1)^2},\\
(\sinh c)^2 &= \frac{4Z}{(\alpha-1)^2(\beta-1)^2}.
\end{aligned}$$

Thus,

$$\begin{aligned}
\frac{\sinh^2(a)}{\sinh^2(c)} &= \frac{\sinh^2(\alpha)}{\sinh^2(\gamma)}\\
&\iff \left[\frac{4X}{(\beta-1)^2(\gamma-1)^2}\right]\left[\frac{(\alpha-1)^2(\beta-1)^2}{4Z}\right] = \left[\frac{(\alpha-1)^2}{-4\alpha}\right]\left[\frac{-4\gamma}{(\gamma-1)^2}\right]\\
&\iff \frac{X(\alpha-1)^2}{Z(\gamma-1)^2} = \frac{\gamma(\alpha-1)^2}{\alpha(\gamma-1)^2} \iff \frac{X}{Z} = \frac{\gamma}{\alpha}.
\end{aligned}$$

Let

$$\begin{aligned} M &= (\beta+\gamma)(1+\beta\gamma)+(\alpha+1)^2\left(\frac{\beta\gamma}{\alpha}\right), \\ N &= (\alpha+\beta)(1+\alpha\beta)+(\gamma+1)^2\left(\frac{\alpha\beta}{\gamma}\right), \\ R &= -(\alpha+1)(\beta+1)(\gamma+1)\beta\delta. \end{aligned}$$

Then $X = M+\gamma R$, $Z = N+\alpha R$. So

$$\frac{X}{Z} = \frac{\gamma}{\alpha} \iff \frac{M+\gamma R}{N+\alpha R} = \frac{\gamma}{\alpha} \iff \alpha(M+\gamma R) = \gamma(N+\alpha R)$$

$$\iff \alpha M+\alpha\gamma R = \gamma N+\alpha\gamma R \iff \alpha M = \gamma N.$$

But

$$\begin{aligned} \alpha M &= \alpha[\ (\beta+\gamma)(1+\beta\gamma)+(\alpha+1)^2\left(\frac{\beta\gamma}{\alpha}\right)\ ] \\ &= \alpha[\ \beta+\gamma+\beta^2\gamma+\beta\gamma^2\ ]+\beta\gamma(\alpha+1)(\alpha+1) \\ &= \alpha\beta+\alpha\gamma+\alpha\beta^2\gamma+\alpha\beta\gamma^2+\alpha^2\beta\gamma+2\alpha\beta\gamma+\beta\gamma, \\ \gamma N &= \gamma[\ (\alpha+\beta)(1+\alpha\beta)+(\gamma+1)^2\left(\frac{\alpha\beta}{\gamma}\right)\ ] \\ &= \alpha\gamma+\beta\gamma+\alpha^2\beta\gamma+\alpha\beta^2\gamma+\alpha\beta\gamma^2+2\alpha\beta\gamma+\alpha\beta. \end{aligned}$$

The proof that $\dfrac{\sinh^2(b)}{\sinh^2(c)} = \dfrac{\sinh^2(\beta)}{\sinh^2(\gamma)}$ is analogous. $\square$

Theorem 3.52. *(Second Cosh Law) In (A,B,C),*

$$\sinh^2(a)\sinh^2(b)\cos^2(\gamma) = [\ \cosh(a)\cosh(b)-\cosh(c)\ ]^2.$$

Proof: Now $(\sinh a)^2 = \dfrac{4X}{(\beta-1)^2(\gamma-1)^2}$, $(\sinh b)^2 = \dfrac{4Y}{(\alpha-1)^2(\gamma-1)^2}$

where

$$\begin{aligned} X &= (\beta+\gamma)(1+\beta\gamma)+(\alpha+1)^2\left(\frac{\beta\gamma}{\alpha}\right)-(\alpha+1)(\beta+1)(\gamma+1)\beta\gamma\delta, \\ Y &= (\alpha+\gamma)(1+\alpha\gamma)+(\beta+1)^2\left(\frac{\alpha\gamma}{\beta}\right)-(\alpha+1)(\beta+1)(\gamma+1)\alpha\gamma\delta. \end{aligned}$$

Therefore,

$$\sinh^2(a)\sinh^2(b)\cos^2(\gamma) \quad = \quad \frac{4XY(\gamma+1)^2}{\gamma(\alpha-1)^2(\beta-1)^2(\gamma-1)^4}.$$

Also

$$\begin{aligned}
&(\alpha-1)^2(\beta-1)^2(\gamma-1)^4[\ \cosh(a)\cosh(b)-\cosh(c)\ ]^2 \\
&\quad = \ [-(\beta+1)(\gamma+1) \ + \ 2(\alpha+1)\beta\gamma\delta\ ]\ [\ -(\alpha+1)(\gamma+1) \ + \ 2(\beta+1)\alpha\gamma\delta\ ] \\
&\qquad - \ [-(\alpha+1)(\beta+1) \ + \ 2(\gamma+1)\alpha\beta\delta\ ](\gamma-1)^2 \ \ )^2 \\
&\quad = (\ (\alpha+1)(\beta+1)(\gamma+1)^2 \ - \ 2\beta\gamma\delta(\alpha+1)^2(\gamma+1) \ - \ 2\alpha\gamma\delta(\beta+1)^2(\gamma+1) \\
&\qquad + \ 4\gamma(\alpha+1)\beta+1) \ + \ (\alpha+1)(\beta+1)(\gamma-1)^2 \\
&\qquad - \ 2\alpha\beta\delta(\gamma+1)(\gamma-1)^2 \ \ )^2 \\
&\quad = \ (\ (\alpha+1)(\beta+1)[\ (\gamma+1)^2+(\gamma-1)^2+4\gamma\ ] \ - \ 2\delta(\gamma+1)[\ \beta\gamma(\alpha+1)^2 \\
&\qquad + \ \alpha\gamma(\beta+1)^2+\alpha\beta(\gamma-1)^2] \ \ )^2.
\end{aligned}$$

Since $(\gamma+1)^2+(\gamma-1)^2+4\gamma \ = \ 2(\gamma+1)^2$,

$$\begin{aligned}
&(\alpha-1)^2(\beta-1)^2(\gamma-1)^4[\ \cosh(a)\cosh(b)-\cosh(c)\ ]^2 \\
&\qquad = \ 4(\gamma+1)^2[\ (\alpha+1)(\beta+1)(\gamma+1) \\
&\qquad\quad -\delta(\ \beta\gamma(\alpha+1)^2 \ + \ \alpha\gamma(\beta+1)^2 \ + \ \alpha\beta(\gamma-1)^2\ )\ \ ]^2.
\end{aligned}$$

Let $W \ = \ (\ \beta\gamma(\alpha+1)^2 \ + \ \alpha\gamma(\beta+1)^2 \ + \ \alpha\beta(\gamma-1)^2\ \ )$. Then

$$\begin{aligned}
\sinh^2(a)\sinh^2(b)\cos^2(\gamma) \quad &= \quad [\ \cosh(a)\cosh(b)-\cosh(c)\ ]^2 \\
\iff \quad XY \ &= \ \gamma[\ (\alpha+1)(\beta+1)(\gamma+1)-\delta W\ ]^2 \\
\iff \quad XY \ &\overset{(1)}{=} \ \gamma[\ (\alpha+1)^2(\beta+1)^2(\gamma+1)^2 \\
&\qquad -2\delta(\alpha+1)(\beta+1)(\gamma+1)W+\delta^2W^2\ ].
\end{aligned}$$

But

$$
\begin{aligned}
XY \;=\; & [\, (\beta+\gamma)(1+\beta\gamma) + (\alpha+1)^2 \left(\frac{\beta\gamma}{\alpha}\right) \;-\; (\alpha+1)(\beta+1)(\gamma+1)\beta\gamma\delta \,] \\
& * \;\; [\, (\alpha+\gamma)(1+\alpha\gamma) \;+\; (\beta+1)^2 \left(\frac{\alpha\gamma}{\beta}\right) \;-\; (\alpha+1)(\beta+1)(\gamma+1)\alpha\gamma\delta \,] \\
=\; & (\alpha+\gamma)(\beta+\gamma)(1+\beta\gamma)(1+\alpha\gamma) \;+\; (\beta+\gamma)(1+\beta\gamma)(\beta+1)^2 \left(\frac{\alpha\gamma}{\beta}\right) \\
& - \;\; (\alpha+1)(\beta+1)(\gamma+1)(\beta+\gamma)(1+\beta\gamma)\alpha\gamma\delta \\
& + \;\; (\alpha+1)(\alpha+\gamma)(1+\alpha\gamma)\left(\frac{\beta\gamma}{\alpha}\right) \;+\; (\alpha+1)^2(\beta+1)^2\gamma^2 \\
& - \;\; (\alpha+1)^3(\beta+1)(\gamma+1)\beta\gamma^2\delta \\
& - \;\; (\alpha+1)(\beta+1)(\gamma+1)(\alpha+\gamma)(1+\alpha\gamma)\beta\gamma\delta \\
& - \; (\alpha+1)(\beta+1)^3(\gamma+1)\alpha\gamma^2\delta \;+\; (\alpha+1)^2(\beta+1)^2(\gamma+1)^2\gamma,
\end{aligned}
$$

$$
\begin{aligned}
W^2 \;=\; & [\, (\beta\gamma(\alpha+1)^2 \;+\; \alpha\gamma(\beta+1)^2 \;+\; \alpha\beta(\gamma-1)^2) \,]^2 \\
=\; & \beta^2\gamma^2(\alpha+1)^4 \;+\; \alpha\beta\gamma^2(\alpha+1)^2(\beta+1)^2 \;+\; \alpha\beta^2\gamma(\alpha+1)^2(\gamma-1)^2 \\
& + \;\; \alpha\beta\gamma^2(\alpha+1)^2(\beta+1)^2 \;+\; \alpha^2\gamma^2(\beta+1)^4 \;+\; \alpha^2\beta\gamma(\beta+1)^2(\gamma-1)^2 \\
& + \;\; \alpha\beta^2\gamma(\alpha+1)^2(\gamma-1)^2 \;+\; \alpha^2\beta\gamma(\beta+1)^2(\gamma-1)^2 \;+\; \alpha^2\beta^2(\gamma-1)^4,
\end{aligned}
$$

$$
\begin{aligned}
\delta^2 W^2 \;=\; & \left(\frac{\beta\gamma}{\alpha}\right)(\alpha+1)^4 \;+\; \left(\frac{\alpha\gamma}{\beta}\right)(\beta+1)^4 \;+\; \left(\frac{\alpha\beta}{\gamma}\right)(\gamma-1)^4 \\
& + \;\; 2\alpha(\beta+1)^2(\gamma-1)^2 \;+\; 2\beta(\alpha+1)^2(\gamma-1)^2 \;+\; 2\gamma(\alpha+1)^2(\beta+1)^2,
\end{aligned}
$$

$$\gamma[\ (\alpha+1)^2(\beta+1)^2(\gamma+1)^2 - 2\delta(\alpha+1)(\beta+1)(\gamma+1)W + \delta^2 W^2\ ]$$

$$\begin{aligned}
&= \boldsymbol{\gamma(\alpha+1)^2(\beta+1)^2(\gamma+1)^2} \ - \ \boldsymbol{2\beta\gamma^2\delta(\alpha+1)^3(\beta+1)(\gamma+1)} \\
&- \ \boldsymbol{2\alpha\gamma^2\delta(\alpha+1)(\beta+1)^3(\gamma+1)} \ - \ 2\alpha\beta\gamma\delta(\alpha+1)(\beta+1)(\gamma+1)(\gamma-1)^2 \\
&+ \ \left(\frac{\beta\gamma^2}{\alpha}\right)(\alpha+1)^4 \ + \ \left(\frac{\alpha\gamma^2}{\beta}\right)(\beta+1)^4 \ + \ \alpha\beta(\gamma-1)^4 \\
&+ \ 2\alpha\gamma(\beta+1)^2(\gamma-1)^2 \ + \ 2\beta\gamma(\alpha+1)^2(\gamma-1)^2 \\
&+ \ \boldsymbol{2\gamma^2(\alpha+1)^2(\beta+1)^2}.
\end{aligned}$$

Thus, (1) holds if and only if

$$\begin{aligned}
&(\alpha+\gamma)(\beta+\gamma)(1+\beta\gamma)(1+\alpha\gamma) \ + \ (\beta+\gamma)(1+\beta\gamma)(\beta+1)^2\left(\frac{\alpha\gamma}{\beta}\right) \\
&\quad - \ (\alpha+1)(\beta+1)(\gamma+1)(\beta+\gamma)(1+\beta\gamma)\alpha\gamma\delta \\
&\quad + \ (\alpha+1)(\alpha+\gamma)(1+\alpha\gamma)\left(\frac{\beta\gamma}{\alpha}\right) \\
&\quad - \ (\alpha+1)(\beta+1)(\gamma+1)(\alpha+\gamma)(1+\alpha\gamma)\beta\gamma\delta \\
&\overset{(2)}{=} \ -\beta\gamma^2\delta(\alpha+1)^3(\beta+1)(\gamma+1) \ - \ \alpha\gamma^2\delta(\alpha+1)(\beta+1)^3(\gamma+1) \\
&\quad - \ 2\alpha\beta\gamma\delta(\alpha+1)(\beta+1)(\gamma+1)(\gamma-1)^2 \ + \ \left(\frac{\beta\gamma^2}{\alpha}\right)(\alpha+1)^4 \\
&\quad + \ \left(\frac{\alpha\gamma^2}{\beta}\right)(\beta+1)^4 \ + \ \alpha\beta(\gamma-1)^4 \\
&\quad + \ 2\alpha\gamma(\beta+1)^2(\gamma-1)^2 \ + \ 2\beta\gamma(\alpha+1)^2(\gamma-1)^2 \ + \ \gamma^2(\alpha+1)^2(\beta+1)^2.
\end{aligned}$$

Note that

$$-(\alpha+1)(\beta+1)(\gamma+1)(\beta+\gamma)(1+\beta\gamma)\alpha\gamma\delta$$

$$-(\alpha+1)(\beta+1)(\gamma+1)(\alpha+\gamma)(1+\alpha\gamma)\beta\gamma\delta$$

$$= \quad -\gamma\delta(\alpha+1)(\beta+1)(\gamma+1)[\ \alpha(\beta+\gamma)(1+\beta\gamma)+\beta(\alpha+\gamma)(1+\alpha\gamma)\ ]$$

$$= \quad -\gamma\delta(\alpha+1)(\beta+1)(\gamma+1)[\ 2\alpha\beta+\alpha\gamma+\beta\gamma+\alpha\beta^2\gamma+2\alpha\beta\gamma^2+\alpha^2\beta\gamma\ ],$$

$$-\beta\gamma^2\delta(\alpha+1)^3(\beta+1)(\gamma+1)\ -\ \alpha\gamma^2\delta(\alpha+1)(\beta+1)^3(\gamma+1)$$

$$-\ 2\alpha\beta\gamma\delta(\alpha+1)(\beta+1)(\gamma+1)(\gamma-1)^2$$

$$= \quad -\gamma\delta(\alpha+1)(\beta+1)(\gamma+1)[\ \beta\gamma(\alpha+1)^2\ +\ \alpha\gamma(\beta+1)^2\ +\ 2\alpha\beta(\gamma-1)^2\ ]$$

$$= \quad -\gamma\delta(\alpha+1)(\beta+1)(\gamma+1)[\ \alpha^2\beta\gamma+\beta\gamma+\alpha\beta^2\gamma+\alpha\gamma+2\alpha\beta\gamma^2+2\alpha\beta\ ].$$

Therefore, (2) holds if and only if

$$(\alpha+\gamma)(\beta+\gamma)(1+\beta\gamma)(1+\alpha\gamma)+\frac{\alpha\gamma}{\beta}(\beta+\gamma)(1+\beta\gamma)(\beta+1)^2$$

$$+(\alpha+1)(\alpha+\gamma)(1+\alpha\gamma)\left(\frac{\beta\gamma}{\alpha}\right)$$

$$=\left(\frac{\beta\gamma^2}{\alpha}\right)(\alpha+1)^4\ +\ \left(\frac{\alpha\gamma^2}{\beta}\right)(\beta+1)^4\ +\ \alpha\beta(\gamma-1)^4\ +\ 2\alpha\gamma(\beta+1)^2(\gamma-1)^2$$

$$+\ 2\beta\gamma(\alpha+1)^2(\gamma-1)^2\ +\ \gamma^2(\alpha+1)^2(\beta+1)^2$$

$$\Longleftrightarrow \quad (\beta+\gamma)(1+\beta\gamma)[\ (\alpha+\gamma)(1+\alpha\gamma)\ +\ \frac{\alpha\gamma}{\beta}(\beta+1)^2\ ]$$

$$+\ \frac{\beta\gamma}{\alpha}(\alpha+1)^2(\alpha+\gamma)(1+\alpha\gamma)$$

$$\stackrel{(3)}{=} \quad \gamma^2(\alpha+1)^2[\ \frac{\beta}{\alpha}(\alpha+1)^2+(\beta+1)^2\ ]\ +\ \alpha\gamma(\beta+1)^2[\ \frac{\gamma}{\beta}(\beta+1)^2$$

$$+\ 2(\gamma-1)^2\ ]+\beta(\gamma-1)^2[\ \alpha(\gamma-1)^2+2\gamma(\alpha-1)^2\ ].$$

The left hand side of (3) is

$$(\beta+\gamma+\beta^2\gamma+\beta\gamma^2)[\ \alpha+\gamma+\alpha^2\gamma+\alpha\gamma^2+\alpha\beta\gamma+2\alpha\gamma+\frac{\alpha\gamma}{\beta}\ ]$$

$$+\ \frac{\beta\gamma}{\alpha}[\ \alpha^3+\alpha^2\gamma+\alpha^4\gamma+\alpha^3\gamma^2+2\alpha^2+2\alpha\gamma+2\alpha^3\gamma+2\alpha^2\gamma^2+\alpha+\gamma+\alpha^2\gamma+\alpha\gamma^2\ ]$$

$$\overset{(4)}{=}\ \gamma^2+\alpha\beta+2\beta\gamma+2\alpha\gamma+2\alpha\gamma^3+2\beta\gamma^3+\alpha^2\gamma^2+\beta^2\gamma^2+2\alpha\gamma^2+2\beta\gamma^2$$

$$+\ \frac{\alpha\gamma^2}{\beta}+\frac{\beta\gamma^2}{\alpha}+2\alpha^2\beta\gamma+6\alpha\beta\gamma^2+2\alpha\beta^2\gamma+4\alpha\beta\gamma+\alpha^2\beta^2\gamma^2$$

$$+\ 2\alpha\beta^2\gamma^3+\alpha\beta^3\gamma^2+2\alpha\beta^2\gamma^2+2\alpha^2\beta\gamma^3+\alpha\beta\gamma^4+4\alpha\beta\gamma^3+\alpha^3\beta\gamma^2+2\alpha^2\beta\gamma^2.$$

The right hand side of (3) is

$$\gamma^2(\alpha^2+2\alpha+1)[\ \alpha\beta+2\beta+\frac{\beta}{\alpha}+\beta^2+2\beta+1\ ]$$

$$+\ \alpha\gamma(\beta^2+2\beta+1)[\ \beta\gamma+2\gamma+\frac{\gamma}{\beta}+2\gamma^2-4\gamma+2\ ]$$

$$+\ \beta(\gamma^2-2\gamma+1)[\ \alpha\gamma^2-2\alpha\gamma+\alpha+2\alpha^2\gamma+4\alpha\gamma+2\gamma\ ]$$

$$\overset{(5)}{=}\ \gamma^2[\ \ (\alpha^3\beta+2\alpha^2\beta+\alpha\beta+\alpha^2\beta^2+2\alpha^2\beta+\alpha^2)\ +\ (2\alpha^2\beta+4\alpha\beta+2\beta+2\alpha\beta^2+4\alpha\beta$$

$$+\ 2\alpha)\ +\ (\alpha\beta+2\beta+\frac{\beta}{\alpha}+\beta^2+2\beta+1)]$$

$$+\ \alpha\gamma[\ \ (\beta^3\gamma+2\beta^2\gamma+\beta\gamma+2\beta^2\gamma^2-4\beta^2\gamma+2\beta^2)\ +\ (2\beta^2\gamma+4\beta\gamma+2\gamma+4\beta\gamma^2$$

$$-\ 8\beta\gamma+4\beta)\ +\ (\beta\gamma+2\gamma+\frac{\gamma}{\beta}+2\gamma^2-4\gamma+2)\ ]$$

$$+\ \beta[(\alpha\gamma^4-2\alpha\gamma^3+\alpha\gamma^2+2\alpha^2\gamma^3+4\alpha\gamma^3+2\gamma^3)\ -\ (2\alpha\gamma^3+4\alpha\gamma^2-2\alpha\gamma$$

$$-\ 4\alpha^2\gamma^2-8\alpha\gamma^2-4\gamma^2)\ +\ (\alpha\gamma^2-2\alpha\gamma+\alpha+2\alpha^2\gamma+4\alpha\gamma+2\gamma)\ ]$$

$$=\ \gamma^2[\alpha^3\beta+\alpha^2\beta^2+6\alpha^2\beta+\alpha^2+2\alpha\beta^2+10\alpha\beta+2\alpha+\beta^2+6\beta+\frac{\beta}{\alpha}+1\ ]$$

$$+\ \alpha\gamma[\ \ \beta^3\gamma+2\beta^2\gamma^2+2\beta^2+4\beta\gamma^2-2\beta\gamma+4\beta+2\gamma^2+\frac{\gamma}{\beta}+2\ ]$$

$$+\ \beta[2\alpha^2\gamma^3-4\alpha^2\gamma^2+2\alpha^2\gamma+\alpha\gamma^4-2\alpha\gamma^2+\alpha+2\gamma^3-4\gamma^2+2\alpha\ ].$$

Expanding and simplifying the right hand side of (5), we get (4). $\square$

4. The Geometry of $PSL_2(\mathbb{E})$ and $PSL_2(\mathbb{F})$.

In this section we consider the actions of $PSL_2(\mathbb{E})$ and $PSL_2(\mathbb{F})$ on $\mathbb{P}^1_{\mathbb{E}}$.

Theorem 4.1. *An extended line L is in the $PSL_2(\mathbb{E})$ orbit of $\widehat{\mathbb{F}}$ if and only if $den(\widehat{\mathbb{F}}, L) \in \mathbb{S}_+$.*

Proof: Assume $g(\widehat{\mathbb{F}}) = L$ where $g(z) = \dfrac{az+b}{cz+d}$, $ad - bc = 1$. If $g^{-1}(\infty) = \dfrac{-d}{c} = \infty$, then $g(z) = a^2 z + \dfrac{b}{d}$ since $ad = 1$.

Thus, $\text{den}(\widehat{\mathbb{F}}, L) = \dfrac{a^2}{\overline{(a^2)}} = \left(\dfrac{a}{\overline{a}}\right)^2 \in \mathbb{S}_+$ since $a^2 + \dfrac{b}{d}, \dfrac{b}{d} \in L$. If $g^{-1}(\infty) \neq \infty$, then $\dfrac{-d}{c} \in \mathbb{F}$ and $h(z) = \dfrac{-1}{z + \frac{d}{c}} \in PSL_2(\mathbb{F})$. Since $g \circ h^{-1}(\widehat{\mathbb{F}}) = L$ and $g \circ h^{-1}(\infty) = \infty$, applying the above argument to $g \circ h^{-1}$ yields the result.

Conversely, assume $\text{den}(\widehat{\mathbb{F}}, L) = r^2$, $r \in \mathbb{S}$. If $L = \widehat{\mathbb{F}+b}$, then $k(z) = z + b \in PSL_2(\mathbb{E})$ and $k(\widehat{\mathbb{F}}) = L$. Thus, we may assume $0 \in L \cap \mathbb{F}$. Now

$$den(\mathbb{F}, (r-1)^2\mathbb{F}) = \rho((r-1)^2) = \frac{r^2 - 2r + 1}{\overline{r}^2 - 2\overline{r} + 1} = r^2$$

since $r \in S$. Since $(r-1)^2\mathbb{F}$ and $L - \{\infty\}$ are both lines through 0 making dengle r^2 with $\mathbb{F}$, $L = ((r-1)^2\mathbb{F}) \cup \{\infty\} = (r-1)^2\widehat{\mathbb{F}}$. □

Corollary 4.2.

i) $\widehat{\mathbb{F}}$ *and* $\widehat{\mathbb{I}}$ *are in the same $PSL_2(\mathbb{E})$ orbit if and only if $\mathbb{I} \cap \mathbb{S} \neq \emptyset$.*

ii) *If $\mathbb{I} \cap \mathbb{S} \neq \emptyset$, then $\mathbb{S}$ and $\mathbb{I}$ (hence $\mathbb{S}$ and $\mathbb{F}$) are in the same $PSL_2(\mathbb{E})$ orbit.*

Proof: i) By Theorem 4.1, $\widehat{\mathbb{F}}$ and $\widehat{\mathbb{I}}$ are in the same $PSL_2(\mathbb{E})$ orbit if and only if $-1 \in S_+$. If $\alpha \in \mathbb{I} \cap \mathbb{S}$, then $-\alpha = \overline{\alpha} = \dfrac{1}{\alpha}$ and $-1 = \alpha^2$. Conversely, if $-1 = \alpha^2$ for $\alpha \in \mathbb{S}$, then $\overline{\alpha} = \dfrac{1}{\alpha} = -\alpha$ and $\alpha \in \mathbb{I} - \{0\}$.

ii) Let $t \in \mathbb{I} \cap \mathbb{S}$. Then $-1 = t^2 \in \mathbb{S}_+$ by the proof of i). Let $t \neq p \in \mathbb{I} \cap \mathbb{S}$. Since $PSL_2(\mathbb{E})$ acts transitively on $\mathbb{P}^1_{\mathbb{E}}$, there exists $g \in PSL_2(\mathbb{E})$ such that $g(p) = \infty$. Thus, den($g(\widehat{\mathbb{I}})$, $g(\mathbb{S})$, $g(t)$) = den($\widehat{\mathbb{I}}$, $\mathbb{S}$, t) = -1 and $g(\widehat{\mathbb{I}})$, $g(\mathbb{S})$ are in the same $PSL_2(\mathbb{E})$ orbit by Theorem 4.1. □

Lemma 4.3. *If $\mathbb{F}$ is finite, $\mathbb{I} \cap \mathbb{S} \neq \emptyset$ if and only if $-1 \notin \mathbb{F}_+$.*

Proof: Since $\mathbb{F}$ is finite, $-1 \in \mathbb{F}^\times \subseteq \mathbb{E}_+$. Thus, $-1 = \alpha^2$, $\alpha \in \mathbb{E}$. Then $\alpha^2 = -1 = \overline{\alpha}^2$ and $\overline{\alpha} = \pm\alpha$. Since $-\alpha = \dfrac{1}{\alpha}$, $\alpha \in \mathbb{F}$ or $\alpha \in \mathbb{I} \cap \mathbb{S}$. Thus, if $-1 \notin \mathbb{F}_+$, then $\alpha \in \mathbb{I} \cap \mathbb{S} \neq \emptyset$.

Conversely, if $t \in \mathbb{I} \cap \mathbb{S}$, then $t^2 = -1$. Since $\pm\, t \in \mathbb{I} - \{0\}$ are the only roots of -1 in $\mathbb{E}$ and $(\mathbb{I} - \{0\}) \cap \mathbb{F} = \emptyset$, $-1 \notin \mathbb{F}_+$. □

Lemma 4.4. *Let C be a Euclidean circle. If N is onto and $sqr(C) \in \mathbb{F}_+$, then C is in the same $PSL_2(\mathbb{E})$ orbit as $\widehat{\mathbb{F}}$.*

Proof: We may assume $C = a\mathbb{S}$. Assume $a\overline{a} = r^2$, $r \in \mathbb{F}^\times$. Since $\mathbb{F}^\times = \mathrm{Im}(N)$, there exists $b \in \mathbb{E}$ with $b\overline{b} = r$. Since $b^2\mathbb{S}$ is a circle centered at 0 with sqradius $(b\overline{b})^2 = r^2 = a\overline{a}$, $b^2\mathbb{S} = a\mathbb{S}$. But $(z \mapsto b^2 z) \in PSL_2(\mathbb{E})$. □

Proposition 4.5. *Let C be a Euclidean circle. If $\mathbb{F}$ is finite and $-1 \notin \mathbb{F}_+$, then C is in the $PSL_2(\mathbb{E})$ orbit of $\widehat{\mathbb{F}}$ if and only if $sqr(C) \in \mathbb{F}_+$.*

Proof: Since C is in the $PSL_2(\mathbb{E})$ orbit of $\widehat{\mathbb{F}}$ and $-1 \notin \mathbb{F}_+$, there exists $g(z) = \dfrac{az+b}{cz+d}$ with $ad - bc = 1$ and $g(\mathbb{S}) = C$. Since $PSL_2(\mathbb{F})$ acts transitively on $\mathbb{H}$ when $\mathbb{F}$ is finite, $\phi PSL_2(\mathbb{F})\phi^{-1} \subseteq U \cap PSL_2(\mathbb{E})$ acts transitively on $\mathbb{P}^1_{\mathbb{E}} - \mathbb{S}$. Thus, we may assume $g^{-1}(\infty) = \infty$. Consequently, $g(z) = a^2 z + \dfrac{b}{d}$, $C = a^2\mathbb{S} + \dfrac{b}{d}$ and $\mathrm{sqr}(C) = (a\overline{a})^2 \in \mathbb{F}_+$. □

Definition: For $g(z) = \dfrac{az+b}{cz+d} \in PSL_2(\mathbb{E})$ with $g(\infty) \neq \infty$, the **isometric circle of** g is $I(g) = \{\ z \in \mathbb{E} \mid\ |z - \left(\frac{-d}{c}\right)|^2 \ = \ \dfrac{1}{|c|^2}\ \}$ (i.e., the circle centered at $g^{-1}(\infty)$ with sqradius $\dfrac{1}{|c|^2}$).

Lemma 4.6. *If $g \in PSL_2(\mathbb{E})$ with $g(\infty) \neq \infty$, then $g(\ I(g)\ ) = I(g^{-1})$.*

Proof: Let $g(z) = \dfrac{az+b}{cz+d}$. Then $I(g^{-1}) = \{\ z \in \mathbb{E} \mid |z - \left(\dfrac{a}{c}\right)|^2 \ = \ \dfrac{1}{|c|^2}\ \}$. If $z \in I(g)$, then $|cz+d|^2 = 1$. Thus,

$$|\ g(z) - \frac{a}{c}\ |^2 \ = \ |\ \frac{az+b}{cz+d} - \frac{a}{c}\ |^2 \ = \ |\ \frac{bc-ad}{c(cz+d)}\ |^2 \ = \ \frac{1}{|c|^2}$$

and $g(\ I(g)\ ) \subseteq I(g^{-1})$. Switching the roles of g and g^{-1} gives $g^{-1}(\ I(g^{-1})\ ) \subseteq I(g)$, hence $I(g^{-1}) \subseteq g(\ I(g)\ )$. □

Theorem 4.7. *Every element g of $PSL_2(\mathbb{E})$ is a product of (at most) four reflections/inversions.*

Proof: Conjugating if necessary, we may assume $g(\infty) \neq \infty$.

Case 1. $I(g) = I(g^{-1})$ (Equivalently, $g^{-1}(\infty) = g(\infty)$)

Choose $x \in I(g)$ such that $g(x) \neq x$. Let M be the perpendicular bisector of the line through x and $g(x)$. Note that M passes through $g^{-1}(\infty)$. (Either $g^{-1}(\infty) = \dfrac{x+g(x)}{2}$ or $M = (g^{-1}(\infty))\left(\dfrac{x+g(x)}{2}\right)$ by Lemma 1.32(i).) Since $r_M(x) = g(x)$, we have $r_M \circ r_{I(g)}(g^{-1}(\infty)) = r_M(\infty) = \infty$, $r_M \circ r_{I(g)}(\infty) = r_M(g^{-1}(\infty)) = g^{-1}(\infty)$, and $r_M \circ r_{I(g)}(x) = r_M(x) = g(x)$. Thus, $r_M \circ r_{I(g)}$, g are elements of $PGL_2(\mathbb{E})$ agreeing on three distinct points. Consequently, $g = r_M \circ r_{I(g)}$.

Case 2. $I(g) \neq I(g^{-1})$.

Let N be the perpendicular bisector of the line through $g(\infty)$, $g^{-1}(\infty)$. Let $x \in I(g)$. By Lemma 1.32(iii), $r_N(x) \in I(g^{-1})$. Thus, $r_N \circ r_{I(g)}(x)$, $g(x) \in I(g^{-1})$. Let $p \in B$ be the rotation with respect to $I(g^{-1})$ such that $p(r_N \circ r_{I(g)}(x)) = g(x)$. Since $p \circ r_N \circ r_{I(g)}(g^{-1}(\infty)) = \infty$ and $p \circ r_N \circ r_{I(g)}(\infty) = g(\infty)$, $p \circ r_N \circ r_{I(g)}$ and g agree on three distinct points and are thus equal. But p is a product of two reflections by Corollary 1.34. $\square$

We now further investigate the structure of $PSL_2(\mathbb{F})$.

Choose $\alpha \in \mathbb{I} - \{0\}$. Then $-\beta = \alpha^2 \in \mathbb{F} - \mathbb{F}_+$ ($-\alpha\overline{\alpha} = \alpha^2 \in \mathbb{F}^\times$. Moreover, $\alpha^2 = a^2$, $a \in \mathbb{F}^\times \implies \alpha = \pm a \implies \alpha \in \mathbb{F}^\times$, a contradiction.) Therefore, $f(x) = x^2 + \beta$ is irreducible over $\mathbb{F}$ and

$$\mathbb{E} = \mathbb{F}[x]/_{\langle f(x) \rangle} \cong \mathbb{F} \oplus \mathbb{F}\alpha.$$

Let

$$P = \{ z + b \mid b \in \mathbb{F} \} \cong \mathbb{F},$$

$$A = PGL_2(\mathbb{F})_0 \cap PGL_2(\mathbb{F})_\infty = \{ az \mid a \in \mathbb{F}^\times \} \cong \mathbb{F}^\times,$$

$$A_+ = PSL_2(\mathbb{F})_0 \cap PSL_2(\mathbb{F})_\infty = \{ az \mid a \in \mathbb{F}_+ \} \cong \mathbb{F}_+$$

$$C = PGL_2(\mathbb{F})_\alpha = \left\{ \begin{bmatrix} a & -b\beta \\ b & a \end{bmatrix} \mid a \in \mathbb{F},\ b \in \mathbb{F},\ a \neq 0 \text{ or } b \neq 0 \right\},$$

$$C_+ = PSL_2(\mathbb{F})_\alpha.$$

Then

$$PGL_2(\mathbb{F})_\infty = \{ az + b \mid a \in \mathbb{F}_\times,\ b \in \mathbb{F} \} = AP,$$

$$PSL_2(\mathbb{F})_\infty = \{ az + b \mid a \in \mathbb{F}_+,\ b \in \mathbb{F} \} = A_+P.$$

Notation: Let $\{1\} \neq K \leq H \leq G$. The **normalizer** of K in H is denoted $N_H(K)$ and the normalizer of K in G is denoted $N(H)$.

Let $h \in P$ and $g \in N_{PGL_2(\mathbb{F})}(P)$. Then $ghg^{-1} \in P$. In particular, $ghg^{-1}(\infty) = \infty$ implies $h(\ g^{-1}(\infty)\ ) = g^{-1}(\infty)$. Therefore, $g^{-1}(\infty) = \infty$ (and hence $g(\infty) = \infty$) since h is parabolic with fixed point ∞. Consequently,

$$N_{PGL_2(\mathbb{F})}(P) \ = \ PGL_2(\mathbb{F})_{\infty}.$$

The arguments for the following are analogous:

$$N_{PGL_2(\mathbb{F})}(A) \ = PGL_2(\mathbb{F})_{\{0,\infty\}}, \quad N_{PGL_2(\mathbb{F})}(C) \ = PGL_2(\mathbb{F})_{\{\alpha,\overline{\alpha}\}}$$

$$N_{PSL_2(\mathbb{F})}(A_+) \ = PSL_2(\mathbb{F})_{\{0,\infty\}}, \quad N_{PSL_2(\mathbb{F})}(C_+) \ = PSL_2(\mathbb{F})_{\{\alpha,\overline{\alpha}\}}.$$

Let $f : \mathbb{F}^\times \longrightarrow GL_2(\mathbb{F})$ be given by $f(a+b\alpha) \ = \ \begin{pmatrix} a & -b\beta \\ b & a \end{pmatrix}$.

When $\mathbb{F}$ is finite, $\mathbb{F}^\times$ is cyclic and thus

$$\mathrm{Im}(f) \ = \ \left\{ \begin{pmatrix} a & -b\beta \\ b & a \end{pmatrix} \mid a, b \in \mathbb{F},\ a \neq 0 \text{ or } b \neq 0 \right\}$$

is also cyclic. Since quotients of cyclic groups are cyclic, $C \cong \mathbb{Z}_{q+1}$ and $C_+ \cong \mathbb{Z}_{\frac{q+1}{2}}$.

Let $g : PGL_2(\mathbb{F})_{\{0,\infty\}} \longrightarrow \{\pm 1\}$ be the map sending $h \in PGL_2(\mathbb{F})_{\{0,\infty\}}$ to 1 if h fixes 0 and ∞ and to -1 if h interchanges 0 and ∞.

Note that $\ker(g) = A$ and that g is onto since $\dfrac{-1}{z} \in PGL_2(\mathbb{F})_{\{0,\infty\}}$.

Let $h : PGL_2(\mathbb{F})_{\{\alpha,\overline{\alpha}\}} \longrightarrow \{\pm 1\}$ be the conjugation map.

Then $\ker(h) = C$ and h is onto since $-z \in PGL_2(\mathbb{F})_{\{\alpha,\overline{\alpha}\}}$.

When $\mathbb{F}$ is finite,

$$\frac{\mid PGL_2(\mathbb{F})_{\{0,\infty\}} \mid}{\mid \ker(g) \mid} \ = \ \mid Im(g) \mid.$$

Therefore, $PGL_2(\mathbb{F})_{\{0,\infty\}}$ has order $2(q-1)$. Since

$$D_{q-1} = \left\langle A, \frac{-1}{z} \right\rangle \leq PGL_2(\mathbb{F})_{\{0,\infty\}},$$

we know $PGL_2(\mathbb{F})_{\{0,\infty\}} = D_{q-1}$.

Similarly, $PGL_2(\mathbb{F})_{\{\alpha,\overline{\alpha}\}} = < C, -z > = D_{q+1}$, $PSL_2(\mathbb{F})_{\{0,\infty\}} = D_{\frac{q-1}{2}}$, and $PSL_2(\mathbb{F})_{\{\alpha,\overline{\alpha}\}} = D_{\frac{q+1}{2}}$.

Notation 4.8. Let G be a finite subgroup of $PGL_2(\mathbb{F})$ where $\mathbb{F}$ has characteristic p.

The **parabolic singular set** of G is $\Upsilon = \{ x \in \widehat{\mathbb{F}} \mid G_x \neq \{1\} \}$.

Given $x \in \Upsilon$, let P_x be the set of all parabolics in G fixing x.

The **hyperbolic singular set** of G is $\Lambda = \{ \{x,y\} \subseteq \widehat{\mathbb{F}} \mid x \neq y,\ G_x \cap G_y \neq \{1\} \}$.

Given $\{x,y\} \in \Lambda$,

$$A_{xy} := G_x \cap G_y = G \cap PSL_2(\mathbb{F})_x \cap PSL_2(\mathbb{F})_y,$$

$$N_{xy} := G_{\{x,y\}} = G \cap PSL_2(\mathbb{F})_{\{x,y\}} = N_G(A_{xy}).$$

G acts on $\Lambda(G) := \{ A_{xy} \mid \{x,y\} \in \Lambda \}$ by conjugation.

The **elliptic singular set** of G is $\Xi = \{ z \in \mathbb{H} \mid G_z \neq \{1\} \}$.

Given $z \in \Xi$, let $C_z := G_z = G \cap PSL_2(\mathbb{F})_z$ and $N_z := G_{\{z,\overline{z}\}} = G \cap PSL_2(\mathbb{F})_{\{z,\overline{z}\}}$.

G acts on $\Xi(G) := \{ C_z \mid z \in \Xi \}$ by conjugation.

Remarks 4.9: i) $P_\infty = G \cap P$ (and thus every P_x) is a Sylow p-subgroup of G since $P \cong \mathbb{F}$ is a Sylow p-subgroup of $PSL_2(\mathbb{F})$.

ii) Now A_{xy} is conjugate to the finite subgroup $A_{0\infty}$ of the multiplicative group $A_+ \cong \mathbb{F}_+ \subseteq \mathbb{F}^\times$. Therefore, A_{xy} is cyclic of order relatively prime to p. Moreover, $N_{0\infty} = \left\langle A_{0\infty}, \frac{-1}{z} \right\rangle$ is dihedral when $\frac{-1}{z} \in G$ and $N_{0\infty} = A_{0\infty}$ is cyclic otherwise. Hence, A_{xy} has index one or two in N_{xy}.

iii) Let g be an elliptic element with fixed points $z, \overline{z}$. Now $PSL_2(\mathbb{F})_z \cong C_+$. Working in the disk model, we can conjugate so that the fixed points are 0 and ∞. Therefore, $C_+ \cong PSL_2(\mathbb{F})_z \cong U_0 \cong \mathbb{S} \subseteq \mathbb{E}^\times$. Consequently, C_z is conjugate to a finite subgroup of $\mathbb{E}^\times$ and hence cyclic of order relatively prime to p. Now $N_0 \cong \left\langle C_0, \frac{-1}{z} \right\rangle$ when $\frac{-1}{z} \in G$ and A_0 is self-normalizing otherwise. Hence, C_z has index one or two in N_z.

iv) Analogous arguments to those given in ii) and iii) show that $H \cap A$ and $H \cap C$ are cyclic when H is a finite subgroup of $PGL_2(\mathbb{F})$. Moreover, $H \cap A$ (and similarly $H \cap C$) is either self-normalizing or has index two in its normalizer, a dihedral group.

v) Let $Q = P_\infty$. Now $N_G(Q) = G \cap N(P) = G \cap B_+$ where $B_+ = \{ az+b \mid a \in \mathbb{F}_+,\ b \in \mathbb{F} \}$ is the Borel group. Therefore, $N_G(Q) \cap P = G \cap P = Q$. Since $P,\ N_G(Q) \leq B_+$ with $P \triangleleft B_+$, the Second Isomorphism Theorem gives that

$$N_G(Q) \,/\, Q = N_G(Q) \Big/ P \cap N_G(Q) \cong PN_G(Q) \,/\, P \leq B_+/P \cong A_+.$$

Consequently, $N_G(Q) \,/\, Q$ is isomorphic to a finite subgroup of A_+ and is therefore cyclic with order relatively prime to p. In fact,

$$N_G(Q) \;=\; G \cap PA_+ \;=\; Q(G \cap A_+) \;=\; QA_{0\infty}.$$

Thus, $[\, N_G(Q) : Q \,] = |A_{0\infty}|$.

Theorem 4.10. *Let $\{\pm 1\} \neq H$ be a finite subgroup of $PGL_2(\mathbb{F})$. If H is abelian, then H is either cyclic, a subgroup of P or a subgroup of D_2.*

Proof: Let $1 \neq h \in H$.

If h is parabolic, we may assume $h(z) = z + b$, $b \in \mathbb{F}^\times$. Let $h \neq g \in H$. Since $gh = hg$, $ghg^{-1} = h$ and $g \in PGL_2(\mathbb{F})_\infty$. Therefore, $g(z) = az+c$. But $gh = hg$ implies $a = 1$. Therefore, $H \leq P$.

If h is hyperbolic, we may assume $h(z) = az$. Now $g \in H$ and H abelian implies $g(\ \{0,\infty\}\ ) = \{0,\infty\} \implies g \in \left\langle\ A,\ \dfrac{-1}{z}\ \right\rangle$. Therefore, $g(z) = bz$ or $g(z) = \dfrac{-b}{z}$.

If $g(z) = \dfrac{-b}{z}$, then $a = -1$ since g commutes with h. Therefore, H is a finite subgroup of A or $H \;\leq\; \{\, \pm\, z,\ \pm\, \frac{1}{z}\ \} \;\cong\; D_2$.

If h is elliptic, then by the above either $H \leq D_2$ or all nontrivial elements of H are elliptic. Assume the latter holds and $h(\alpha) = \alpha$. Since H is abelian, $1 \neq g \in H$ implies $g \in H \cap PGL_2(\mathbb{F})_{\{\alpha,\overline{\alpha}\}} \;=\; H \cap \left\langle\ PGL_2(\mathbb{F})_\alpha, -z\ \right\rangle$.

Since g and h are in a dihedral group and h is in the cyclic part of the dihedral group, $gh = h^{-1}g$. Thus, either H is a finite subgroup of C or h has order 2 since g and h commute. In the latter case, H is noncyclic of order 4 (hence isomorphic to D_2). $\square$

We now classify the finite subgroups of $PSL_2(\mathbb{F})$. Dickson solved this problem for $\mathbb{F} = \mathbb{F}_q$ in the early 1900's, though our arguments are more geometric than his. We also count the number of subgroups of $PSL_2(q)$. Modern references don't seem to do this [S].

Notation 4.11. Let $\{1\} \neq G$ be a finite subgroup of $PSL_2(\mathbb{F})$ where the characteristic of $\mathbb{F}$ is p. Let $Q = P \cap G$.

Let $C_1, C_2, \ldots, C_{s+t}$ denote the distinct elements of $[\,\Lambda(G)/G\,] \cup [\,\Xi(G)/G\,]$. Assume that for a representative W_i of C_i,

$$\begin{aligned} N_G(W_i) &= W_i && \text{for } i \leq s, \\ [\,N_G(W_i) : W_i\,] &= 2 && \text{for } i > s. \end{aligned}$$

Let $|G| = g,\ \ |Q| = r,\ \ [\,N_G(Q) : Q\,] = k,\ \ |W_i| = w_i$.

Lemma 4.12. *Let $\{1\} \neq G$ be a finite subgroup of $PSL_2(\mathbb{F})$. Letting s and t be as in*

4.11, one of the following holds:

i) $s = 1,\ t = 0$	*ii)* $s = 1,\ t = 1$	*iii)* $s = 0,\ t = 0$
iv) $s = 0,\ t = 1$	*v)* $s = 0,\ t = 3$	*vi)* $s = 0,\ t = 2$

Proof: The number of nontrivial elements contained in a conjugate of W_i is

$$(|W_i| - 1)|C_i| = (w_i - 1)\left|\frac{G}{N_G(W_i)}\right| = (w_i - 1)\left(\frac{|G|}{\left| [N_G(W_i) : W_i] \, |W_i| \right|}\right)$$

$$= \begin{cases} \dfrac{(w_i - 1)g}{w_i} & \text{if } 1 \leq i \leq j \\ \dfrac{(w_i - 1)g}{2w_i} & \text{otherwise.} \end{cases}$$

Similarly, the number of nontrivial elements found in any conjugate of Q is

$$(|Q| - 1)\left(\frac{g}{rk}\right) = \frac{(r-1)g}{rk}.$$

Since the W_i's together with the Sylow p-subgroups of G form a partition $G - \{1\}$,

$$g - 1 = |G| - 1 = \frac{(r-1)g}{rk} + \sum_{i=1}^{s} \frac{(w_i - 1)g}{w_i} + \sum_{i=s}^{t} \frac{(w_i - 1)g}{2w_i}.$$

Therefore

$$1 = \frac{1}{g} + \frac{r-1}{rk} + \sum_{i=1}^{s} \frac{(w_i - 1)}{w_i} + \sum_{i=s}^{t} \frac{(w_i - 1)}{2w_i}.$$

Now $r = p^m$, $m \in \mathbb{N}$ and w_i is an integer ≥ 2 for all i. Therefore, $\dfrac{w_i - 1}{w_i} \geq \dfrac{1}{2}$ for all i and

$$1 = \underbrace{\frac{1}{g} + \frac{r-1}{rk}}_{>0} + \underbrace{\sum_{i=1}^{s} \frac{(w_i - 1)g}{w_i}}_{\geq \frac{s}{2}} + \underbrace{\sum_{i=s}^{t} \frac{(w_i - 1)g}{2w_i}}_{\geq \frac{t}{4}}.$$

Consequently, $1 > \dfrac{s}{2} + \dfrac{t}{4} \implies s < \dfrac{4-t}{2}$. Therefore $s < 2$. But $s = 0$ implies $0 \leq t \leq 3$ and $s = 1 \implies 0 \leq t \leq 1$. $\square$

Definition: The subgroups of $SO(3)$ of rotational symmetries of the (regular) tetrahedron, octahedron, and icosahedron respectively are called **tetrahedral**, **octahedral**, and **icosahedral** groups.

Note that

$$\mathrm{Alt}(4) \cong PSL_2(3) \cong T_+(2,3,3)$$

are tetrahedral groups,

$$\mathrm{Symm}(4) \cong PGL_2(3) \cong T_+(2,3,4)$$

are octahedral groups, and

$$\mathrm{Alt}(5) \cong PSL_2(4) \cong PSL_2(5) \cong T_+(2,3,5)$$

are icosahedral groups where $T_+(p,q,r)$ denotes the orientation preserving subgroup of the triangle group

$$< s, t, u \mid s^2, t^2, u^2, (st)^p, (tu)^q, (us)^r > .$$

Theorem 4.13. *Let $\{1\} \neq G$ be a finite subgroup of $PSL_2(\mathbb{F})$. Then G is (isomorphic to) one of the following:*

i) *A cyclic subgroup*

ii) *A subgroup of the Borel B_+*

iii) *A dihedral group*

iv) *A tetrahedral, octahedral or icosahedral group*

v) *$PSL_2(p^\ell)$ where $\ell \mid n$ if $\mathbb{F} = \mathbb{F}_{p^n}$*

vi) *$PGL_2(p^\ell)$ where $2\ell \mid n$ if $\mathbb{F} = \mathbb{F}_{p^n}$.*

Proof: We will use the notation of 4.11.

Case 1. $s = 1,\ t = 0$

Now

$$1 = \frac{1}{g} + \frac{r-1}{rk} + \frac{w_1 - 1}{w_1} \implies 1 = \frac{1}{g} + \frac{r}{rk} - \frac{1}{rk} + \frac{w_1}{w_1} - \frac{1}{w_1}$$
$$\implies 0 = \frac{1}{g} + \frac{1}{k} - \frac{1}{rk} - \frac{1}{w_1}.$$

Therefore,

$$\boxed{\frac{1}{rk} + \frac{1}{w_1} = \frac{1}{g} + \frac{1}{k}}$$

If $r = 1$ (i.e., there are no parabolics in G), then $g = w_1$ which implies $G = W_i$ is cyclic.

Assume $r > 1$. If $k = 1$, then we have

$$\underbrace{\frac{1}{r}}_{<\frac{1}{2}} + \underbrace{\frac{1}{w_1}}_{<\frac{1}{2}} = \underbrace{\frac{1}{g}}_{>0} + 1,$$

a contradiction. Therefore $k > 1$. By Remark 4.12(ii), $N_G(Q) = QA_{0\infty}$. Since $s = 1$, $A_{0\infty}$ is conjugate to W_1 and $w_1 = |A_{0\infty}| = k$. Therefore,

$$g = rk = |Q|\ [N_G(Q) : Q] = |N_G(Q)|.$$

I.e., $G = N_G(Q) = G \cap B_+ \leq B_+$.

Case 2. $s = 1,\ t = 1$

Now $1 = \dfrac{1}{g} + \dfrac{r-1}{rk} + \dfrac{w_1 - 1}{w_1} + \dfrac{w_2 - 1}{2w_2} \implies 1 = \dfrac{1}{g} + \dfrac{r-1}{rk} + 1 - \dfrac{1}{w_1} + \dfrac{1}{2} - \dfrac{1}{2w_2}$. Therefore,

$$\boxed{\frac{1}{w_1} + \frac{1}{2w_2} = \frac{1}{2} + \frac{1}{g} + \frac{r-1}{rk}} \tag{14–1}$$

If $r > 1$, then $\dfrac{r-1}{rk} \geq \dfrac{1}{2k}$. Consequently, (14–1) gives

$$\frac{1}{w_1} + \frac{1}{2w_2} \geq \frac{1}{2} + \frac{1}{g} + \frac{1}{2k}$$
$$\Longrightarrow \frac{1}{2w_2} - \frac{1}{2k} \geq \left(\frac{1}{2}+\frac{1}{g}\right) - \frac{1}{w_1} = \underbrace{\frac{1}{g}}_{>0} + \underbrace{\left(\frac{1}{2}-\frac{1}{w_1}\right)}_{\geq 0} > 0.$$

. Therefore, $k > w_2 \geq 2$. Since $N_G(Q) = Q < x >$ where $< x >$ is conjugate to some W_i but $k \neq w_2$, we must have $k = w_1$. But then the equation $\dfrac{1}{2w_2} - \dfrac{1}{2k} \geq \dfrac{1}{2} + \dfrac{1}{g} - \dfrac{1}{w_1}$ implies

$$\underbrace{\frac{1}{2w_2}}_{\leq \frac{1}{4}} + \underbrace{\frac{1}{2w_1}}_{\leq \frac{1}{4}} \geq \frac{1}{2} + \frac{1}{g} > \frac{1}{2},$$

a contradiction. Therefore, $r = 1$ and there are no parabolics in G.

Then $\dfrac{1}{w_1} + \dfrac{1}{2w_2} = \dfrac{1}{2} + \dfrac{1}{g} > \dfrac{1}{2}$ which implies that either $w_1 = 2$ (and $g = 2w_2$) or $w_1 = 3$ ($\Longrightarrow$ $w_2 = 2$ and $g = 12$).

Case 2A. $w_1 = 2$

Now $g = 2w_2 = [N_G(W_2) : W_2]\ |W_2| = |N_G(W_2)|$ and $G = N_G(W_2)$. But $N_G(W_2)$ is dihedral since $[\ N_G(W_2) : W_2\ ] = 2$.

Case 2B. $w_1 = 3$.

Since $|W_2| = 2$ and $[\ N_G(W_2) : W_2\ ] = 2$, $N_G(W_2) = D_2$. Now D_2 contains three elements of order 2, say x_1, x_2, x_3. Also $|C_2| = [G : N_G(W_2)] = \dfrac{12}{4} = 3$. Therefore, $C_2 = \{ < x_1 >, < x_2 >, < x_3 > \}$ since there is only one congugacy class of W_i's with cardinality two. Given $g \in G$ and $x_i \in D_2$, $< g^{-1}xg > \in C_2$ and therefore $g^{-1}x_ig = x_j$ for some $1 \leq j \leq 3$. Hence, $D_2 \triangleleft G$. Since $[G : D_2] =$

$3 = |W_1|$ and there is only one conjugacy class of elements of order 3, G/D_2 is conjugate to (hence isomorphic to) W_1. Consequently, $G = D_2 \rtimes W_1$. I.e., $G \cong \mathrm{Alt}(4)$.

Case 3. $s = 0,\ t = 0$

Since there is no element in G whose order is relatively prime to p and Q is a Sylow p- subgroup of G, we have $G = Q \leq P \leq B$.

Case 4. $s = 0,\ t = 1$

Now

$$1 = \frac{1}{g} + \frac{r-1}{rk} + \frac{w_1 - 1}{2w_1} = \frac{1}{g} + \frac{r-1}{rk} + \frac{1}{2} - \frac{1}{2w_1} \implies \frac{1}{2} + \frac{1}{2w_1} = \frac{1}{g} + \frac{r-1}{rk}.$$

But $g \geq 2w_1 = |N_G(W_1)|$ so $\frac{r-1}{rk} = \frac{1}{2} + \underbrace{\left(\frac{1}{2w_1} - \frac{1}{g}\right)}_{\geq 0} \geq \frac{1}{2}$. So $r > 1$. Also $\underbrace{\left(\frac{r-1}{r}\right) - \left(\frac{1}{k}\right)}_{<1} \geq \frac{1}{2} \implies \frac{1}{k} > \frac{1}{2} \implies k < 2 \implies k = 1$.

Therefore, $Q = N_G(Q)$ and $\frac{1}{2} + \frac{1}{2w_1} = \frac{1}{g} + 1 - \frac{1}{r} \implies \frac{1}{r} + \frac{1}{2w_1} = \frac{1}{2} + \frac{1}{g}$. In particular, $\frac{1}{2} + \frac{1}{2w_1} > \frac{1}{2}$ which implies $r = 2$ or $r = 3$. Since $|Q| = p^m$, $p = 2$ or $p = 3$.

If $r = 2$, then $g = 2w_1 = |N_G(W_1)|$. Consequently, $r = 2$ implies that $p = 2$ and $G = N_G(W_1)$ is a dihedral group.

If $r = 3$, then $\frac{1}{3} + \frac{1}{2w_1} > \frac{1}{2} \implies \frac{1}{2w_1} > \frac{1}{2} - \frac{1}{3} = \frac{1}{6} \implies w_1 < 3$. So $1 < w_1 < 3 \implies w_1 = 2$. Therefore, $\frac{1}{g} = \frac{1}{4} - \frac{1}{6}$ and $g = 12$. Thus, we have $p = 3$, $|G| = 12$, $|W_1| = 2$, $|Q| = 3$. Arguing as in Case 2B, we get that $G \cong \mathrm{Alt}(4)$.

Case 5. $s = 0,\ t = 3$

Now

$$1 = \frac{1}{g} + \frac{r-1}{rk} + \frac{w_1 - 1}{2w_1} + \frac{w_2 - 1}{2w_2} + \frac{w_3 - 1}{2w_3}$$
$$\Longrightarrow\ 1 = \frac{1}{g} + \frac{r-1}{rk} + \frac{3}{2} - \frac{1}{2w_1} - \frac{1}{2w_2} - \frac{1}{2w_3}.$$

Therefore,

$$\boxed{\frac{1}{2w_1} + \frac{1}{2w_2} + \frac{1}{2w_3} = \frac{1}{2} + \frac{1}{g} + \frac{r-1}{rk}} \tag{14–2}$$

If $r > 1$, then $\dfrac{r-1}{rk} \geq \dfrac{1}{2k}$. Consequently, the left hand side of (14–2) is $\leq 3\left(\dfrac{1}{4}\right)$ while the right hand side is $\geq \dfrac{1}{2} + \dfrac{1}{g} + \dfrac{1}{2k} > \dfrac{1}{2} + \dfrac{1}{2k}$. This implies that $k > 1$. But then Remark 4.12(ii) gives that $k = w_i$ for some w_i, say w_1. Then (14–2) gives that

$$\frac{1}{2w_1} + \frac{1}{2w_2} + \frac{1}{2w_3} \geq \frac{1}{2} + \frac{1}{g} + \frac{1}{2w_1}$$
$$\Longrightarrow\ \underbrace{\frac{1}{2w_2} + \frac{1}{2w_3}}_{\leq \frac{1}{2}} \geq \frac{1}{2} + \frac{1}{g} > \frac{1}{2},$$

a contradiction. Hence, $r = 1$ and there are no parabolics in G.

We may assume $w_1 \leq w_2 \leq w_3$. Since $r = 1$, the right hand side of (14–2) is larger than one half. If $w_1 \geq 3$, then so are w_2 and w_3 and the left hand side of (14–2) is $\leq 3\left(\dfrac{1}{6}\right)$, a contradiction. Hence, $w_1 = 2$. In particular,

$$w_1 = 2,\ w_2 = 2,\ g = 2w_3 \qquad \text{or} \qquad w_1 = 2,\ w_2 = 3,\ w_3 \leq 5.$$

(The equation $\dfrac{1}{4} + \dfrac{1}{6} + \dfrac{1}{2w_3} > \dfrac{1}{2}$ implies that $w_3 < 6$. So $w_3 \leq 3$ when $w_1 = 2$ and $w_2 = 3$. If $w_2 > 3$, then $w_3 > 3$ as well and the left hand side of (14–2) is less than one half.)

Case 5A. $w_1 = 2,\ w_2 = 2,\ g = 2w_3$

Since $|G| = |N_G(W_3)|$, G is the dihedral group $N_G(W_3)$.

Case 5B. $w_1 = 2,\ w_2 = 3,\ w_3 = 3$

Then $\dfrac{1}{g} = \dfrac{1}{4} + \dfrac{1}{6} + \dfrac{1}{6} - \dfrac{1}{2}$ by (14–2) and $|G| = 12$. Since $|G| = 2^2 \cdot 3$, W_2 and W_3 are Sylow 3-subgroups of G and are therefore conjugate. Since this is impossible, Case 5B can't happen.

Case 5C. $w_1 = 2,\ w_2 = 3,\ w_3 = 4$

Then $\dfrac{1}{g} = \dfrac{1}{4} + \dfrac{1}{6} + \dfrac{1}{8} - \dfrac{1}{2}$ and $|G| = 24 = 2^3 \cdot 3$. Since $|W_2| = 3$, $N_G(W_2)$ is dihedral of order 6 and $[G : N_G(W_2)] = 4$. Now the only (nontrivial) normal subgroup of $N_G(W_2)$ is W_2. But $|C_2| = [G : N_G(W_2)] = 4 \neq 1$ and W_2 is a Sylow 3-subgroup of G. Hence, W_2 is not normal in G. Therefore, $N_G(W_2)$ is a subgroup of G of index 4 containing no nontrivial normal subgroup of G. Consequently, G is isomorphic to a subgroup of Symm(4). But since the order of G equals the order of Symm(4), G is isomorphic to Symm(4).

Case 5D. $w_1 = 2,\ w_2 = 3,\ w_3 = 5$

Then $\dfrac{1}{g} = \dfrac{1}{4} + \dfrac{1}{6} + \dfrac{1}{10} - \dfrac{1}{2}$ and $|G| = 60 = 2^2 \cdot 3 \cdot 5$. Choose an element $1 \neq g \in N_G(W_1) = D_2$. Given an element h of order 3 in G, $|gh| \in \{2, 3, 5\}$ because $< gh >$ is conjugate to one of the w_i. If $|gh| = 5$, then $< g, h > = T_+(2, 3, 5)$. If $|gh| = 3$, then $< g, h >$ is $T_+(2, 3, 3)$, a subgroup of index 5 in G. Since D_2 is a Sylow 2-subgroup of G and $|C_1| = [G : N_G(W_1)] = 15 \neq 1$, D_2 is not normal in G. Since D_2 is the only nontrivial normal subgroup of Alt(4), $|G|$ is isomorphic to a subgroup of Alt(5) (hence isomorphic to Alt(5)). Consequently,

$G \cong \mathrm{Alt}(5)$ in either case.

We now want to show that there is an $h \in G$ with $|h| = 3$ and $|gh| \neq 2$. If $|x| = 3$ and $|gx| = 2$, then $< g, x >= D_3$. Moreover, $< g >$ normalizes $< x >$ since $gxgx = 1 \implies g^{-1}xg = x^{-1} \in < x >$. By the argument given below, $< g >$ normalizes exactly two subgroups of order three. Consequently, there are four elements of order 3 in G such that $|gx| = 2$ $(< x >=< x^{-1} >)$. But G contains $|C_2| = [G : D_3] = 10$ elements of order 3 and thus such an h always exists.

Let the cyclic subgroups of G of orders 2 and 3 be the vertex set of a graph where subgroups of order 2 are colored red and subgroups of order 3 are colored green. Then there are 10 green vertices and $|C_1| = 15$ red ones. There is an edge between a red vertex $< u >$ and a green vertex $< v >$ if and only if $u^{-1} < v > u = < v >$. G acts on this graph by conjugation.

Let U, V, and E denote the number of red vertices, green vertices, and edges respectively.

Given a green vertex v, $N_G(< v >) = D_3$ contains exactly 3 elements of order 2. Thus, each green vertex forms an edge with exactly three red ones. Thus, $E = 3V = 3(10) = 30$.

On the other hand, G acts transitively on the red vertices and thus all red vertices have the same degree. Thus, $E = U$(degee of each red vertex) and each red vertex has degree $30 \div 15 = 2$.

Case 6. $s = 0, \ t = 2$

Now

$$1 = \frac{1}{g} + \frac{r-1}{rk} + \frac{w_1 - 1}{2w_1} + \frac{w_2 - 1}{2w_2}$$

$$\Longrightarrow 1 = \frac{1}{g} + \frac{r-1}{rk} + \frac{1}{2} - \frac{1}{2w_1} + \frac{1}{2} - \frac{1}{2w_2}.$$

Therefore,

$$\boxed{\frac{1}{2w_1} + \frac{1}{2w_2} = \frac{1}{g} + \frac{r-1}{rk}} \tag{14–3}$$

Since $g \geq 2w_1 = |N_G(W_1)|$, (14–3) implies that $r > 1$ and thus $\frac{r-1}{rk} \geq \frac{1}{2k}$. If $k = 1$, then the right hand side of (14–3) is larger than $\frac{1}{2}$. This is a contradiction since the left hand side of the equation is $\leq \frac{1}{2}$. Thus, $k > 1$ and $k = w_i$ for some i by Remark 4.12(ii). We may assume $k = w_1$. Therefore,

$$\boxed{\frac{1}{2w_1} + \frac{1}{2w_2} = \frac{1}{g} + \frac{1}{w_1} - \frac{1}{rw_1}} \tag{14–4.}$$

Clearing the fractions in (14–4), we get

$$(2w_1w_2rg)\left(\frac{1}{2w_1} + \frac{1}{2w_2}\right) = \left(\frac{1}{g} + \frac{1}{w_1} - \frac{1}{rw_1}\right)(2w_1w_2rg)$$

$$\Longrightarrow w_2rg + w_1rg = 2w_1w_2r + 2w_2rg - 2w_2g$$

$$= 2w_1w_2r + 2w_2g(r-1).$$

Define a by $ag = 2w_1w_2r$. Then cancelling g from the above equation we have $w_1r = a + w_2r - 2w_2$ or

$$\boxed{w_1r = a + w_2(r-2)} \tag{14–5}$$

Let $x \in Q - \{1\}$. Then $Q = C_G(x)$ where $C_G(x)$ is the centralizer of G in x. (Given y distinct from x in $C_G(x)$, $< x, y >$ is abelian and thus contained in Q by Theorem 4.10. Thus, the number of elements in $N_G(Q)$ congugate to

x is $[\, N_G(Q) : C_G(x) \,] = [\, N_G(Q) : Q \,] = k$. Thus, $k = w_1$ divides $r-1$. By (14–5), $w_1 r = (a - w_2) + (r-1)w_2$. Consequently, since $w_1 \mid (r-1)$, w_1 also divides $a - w_2$.

Since $2w_2$ is the order of $N_G(W_2)$, $g = 2w_2 z$ for some $z \in \mathbb{Z}^+$. Therefore, $2w_1 w_2 r = ag = 2aw_2 z \implies az = w_1 r$. I.e., a divides $w_1 r$.

Now $a = w_1 r - w_2(r-2)$. Say $|Q| = p^m$. If p^s divides a for some $s \le m$, then p^s also divides $w_2(r-2)$. Since w_2 and p are relatively prime, $p^s \mid (p^m - 2)$ which implies $p = 2$ and $s = 1$. Thus, $\gcd(a, r) = 2$ if $p = 2$ and 1 otherwise. Consequently, the fact that $a \mid w_1 r$ implies that $a \mid w_1$ or $\frac{a}{2} \mid w_1$. In either case, $a \mid 2w_1$.

By (14–4), $$\frac{1}{2w_2} = \frac{1}{2w_1} + \underbrace{\left(\frac{1}{g} - \frac{1}{rw_1}\right)}_{<0} < \frac{1}{2w_1} \implies w_1 < w_2.$$

Finally, note that $a \in \mathbb{Z}^+$. Therefore, $w_1 = \underbrace{\frac{a}{r}}_{>0} + \frac{w_2(r-2)}{r} > \frac{w_2(r-2)}{r}$.

Case 6A. Assume $r \ge 4$.

Since $r \ge 4$, $w_1 > \dfrac{w_2(r-2)}{r} \implies 2w_1 > w_2$. Since w_1 divides $w_2 - a$, and a divides $2w_1$, write $w_2 = a + \ell w_1$ and $2w_1 = aw$. But

$$w_1 < w_2 < 2w_1 \implies w_1 < \frac{2w_1}{w} + \ell w_1 < 2w_1 \implies 1 < \underbrace{\frac{2}{x}}_{>0} + \ell < 2.$$

Hence, $\ell = 1$ and $w_2 = a + w_1$.

Now by (14–5), $w_1 r = a + (a + w_1)(r-2) \implies w_1 = \left(\dfrac{r-1}{2}\right) a$.
Moreover, $w_2 = a + w_1 = \left(\dfrac{r+1}{2}\right) a$ and $g = \dfrac{2w_1 w_2 r}{a} = \left(\dfrac{r(r^2-1)}{2}\right) a$.

Since $\dfrac{2}{a} = \dfrac{r-1}{w_1}$ and $w_1 \mid (r-1)$, we know that $\dfrac{2}{a} \in \mathbb{Z}^+$. Therefore, $a = 1$ or $a = 2$.

Consequently, when $r \geq 4$ one of the following occurs:

$$\begin{aligned} w_1 &= \frac{r-1}{2}, & w_2 &= \frac{r+1}{2}, & g &= \frac{r(r^2-1)}{2} \\ w_1 &= r-1, & w_2 &= r+1, & g &= r(r^2-1). \end{aligned}$$

Note that $r \neq 2$ since w_1 divides $r-1$. Moreover, if $r = 3$ then $w_1 = 2$ and $2 = w_1 < w_2$. Since we also know that $w_1 > \dfrac{w_2(r-2)}{r}$, $2 < w_2 < 6$. But $\gcd(w_2, 3) = \gcd(w_2, r) = 1$. Consequently, either $r \geq 4$ or $r = 3$, $w_1 = 2$, and $w_2 \in \{4, 5\}$.

Case 6B. $r = 3,\ w_1 = 2,\ w_2 = 4$

Note that $w_1 = r-1$, $w_2 = r+1$, and $g = r(r^2-1)$. I.e., this is a special case of 6A.

Case 6C. $r = 3,\ w_1 = 2,\ w_2 = 5$

Now $a = w_1 r - (r-2)w_2 = 1$ and thus $g = 2w_1w_2r = 60$. Now G acts transitively on its Sylow 2-subgroups by conjugation. Now the Sylow 2-subgroups intersect only at the identity. (If $1 \neq h \in D_2 \cap D_2'$, then $D_2 \leq N(< h >)$. But $N(< h >)$ has order 4 since $s = 0$. Thus, $D_2 = N(< h >)$ and similarly $D_2' = N(< h >)$.) Therefore, there are 5 Sylow 2-subgroups of G since G contains 15 elements of order two. Thus, we have a group homomorphism $\phi : G \longrightarrow \mathrm{Symm}(5)$. Let $g \in \ker(\phi)$. Then $g^{-1}D_2g = D_2$ and $g \in N(D_2)$ for all D_2.

Now $|g| \in \{ 1,2,3,5 \}$. Since there are 5 Sylow 2-subgroups, $5 = [G : N_G(D_2)]$ and $| N_G(D_2) | = 12$. Thus, $|g| \neq 5$.

If $|g| = 2$, then pick D_2 not containing g and consider $H = < D_2, g >$. Since $g \in N(D_2)$, $D_2 \lhd H$ and thus the Third Isomorphism Theorem gives

$$< g > \cong < g > \Big/ < g > \cap D_2 \cong H \,/\, D_2 = < g > D_2 \,/\, D_2$$

Consequently, $|H| = 8$, contradicting that $|G| = 60$.

Thus, $g \in \ker(\phi) \implies |g| \in \{ 1,3 \}$. Given a Sylow 5-subgroup K, $| N_G(K) | = 10$. Since the Sylow 5-subgroups have prime order and thus intersect only at the identity, there are 6 Sylow 5-subgroups and thus 24 elements of order 5. Consequently, there are $60 - 1 - 15 - 24 = 20$ elements of order 3 in G. Since the Sylow 3-subgroups must also be disjoint, there are 10 Sylow 3-subgroups. If $|g| = 3$, then $| N_G(< g >) | = \dfrac{60}{10} = 6$. Consequently, there is an element $h \in N_G(< g >)$ with $|h| = 2$.

Now $h \in N_G(< g >) \implies hgh^{-1} = g$ or $hgh^{-1} = g^{-1}$. If $hgh^{-1} = g$, then g and h commute. But $N_G(< h >) = {D_2}' = \{ 1, h, x, y \}$ for some ${D_2}'$ which g normalizes. Since $< g >$ acts on $\{ h, x, y \}$ by conjugation, the orbit of x in $< g >$ contains either 1 or 3 elements (since its cardinality divides the order of $< g >$). Thus, g commutes with x and hence all of ${D_2}'$. But then ${D_2}' \leq N_G(< g >)$, a contradiction since 4 does not divide 6.

If $hgh^{-1} = g^{-1}$, then $N_G(< g >) = < g, h > \cong D_3$. Since g and h don't commute, the orbit of h in $< g >$ contains 3 elements, namely h, x, y. I.e., ${D_2}' \leq N_G(< g >) = D_3$, a contradiction since 4 does not divide 6.

Consequently, $\ker(\phi) = \{1\}$. Thus, $G \cong \phi(G) \le \mathrm{Symm}(5)$ and $|\phi(G)| = |G| = 60$. Hence, $\phi(G) = \mathrm{Alt}(5)$.

(Note: An argument similar to this one could have been used for Case 5D but we chose to give a different proof for variety.)

It remains to determine the structure of G in Case 6A. Conjugating if necessary, we may assume $Q = G \cap P$. Then $N_G(Q) = Q < wz >$ where $< wz > = G \cap A_+$, $w \in \mathbb{F}_+$. Also $\frac{-1}{z} \in G$ since $N_G(< wz >) = \left\langle G \cap A_+, \frac{-1}{z} \right\rangle$.

If $w_1 = \frac{r-1}{2}$, then $|w| = w_1 = \frac{r-1}{2}$ and $< w > = (\mathbb{F}_r)_+$. Consequently, $\{ az \mid a \in (\mathbb{F}_r)_+ \} = G \cap A_+ \le G$. Likewise, if $w_1 = r-1$, then $|w| = r-1$ and $< w > = (\mathbb{F}_r)^\times$. Consequently, $\{ az \mid a \in (\mathbb{F}_r)^\times \} = G \cap A_+ \le G$.

We now show that $Q = \{ z + b \mid b \in \mathbb{F}_r \}$. For then $PGL_2(r) = \left\langle B(r), \frac{-1}{z} \right\rangle \le G$ when $w_1 = r-1$ where $B(r) = \{ z + b \mid b \in \mathbb{F}_r \} \{ az \mid a \in (\mathbb{F}_r)^\times \}$ is the Borel group in $PGL_2(r)$. Since G and $PGL_2(r)$ both have order $r(r^2-1)$, $G = PGL_2(r)$. Likewise, $G = \left\langle B_+(r), \frac{-1}{z} \right\rangle = PSL_2(r)$ when $w_1 = \frac{r-1}{2}$ where $B_+(r)$ is the Borel group in $PSL_2(r)$.

Let M denote the double coset

$$N_G(Q)\left(\frac{-1}{z}\right)Q = \{ (a^2 z + b)\left(\frac{-1}{z}\right)(z+d) \mid a \in (\mathbb{F}_r)^\times,\ b,d \in \mathbb{F}_r \}.$$

Claim: $G = N_G(Q) \cup M$.

Proof: Now M contains $[\, Q : Q \cap \left[\left(\frac{-1}{z}\right) N_G(Q) \left(\frac{-1}{z}\right)\right] \,]$ cosets of $N_G(Q)$. But $g(z) \in \left(\frac{-1}{z}\right) N_G(Q) \left(\frac{-1}{z}\right) \implies g(z) = \left(\frac{-1}{z}\right)(a^2 z + b)\left(\frac{-1}{z}\right) =$

$\dfrac{z}{-bz+a}$. Either g does not fix ∞, ($b \neq 0$) or $g(z) = \dfrac{z}{a}$ is hyperbolic (fixing 0 and ∞). In either case, $g \notin Q$ and thus $Q \cap \left[\left(\dfrac{-1}{z}\right) N_G(Q) \left(\dfrac{-1}{z}\right)\right] = \emptyset$. Hence, M contains $|Q| = r$ cosets of $N_G(Q)$, each of which contains $|N_G(Q)|$ elements. Therefore,

$$|M| = r|N_G(Q)| = r(\,[N_G(Q):Q]|Q|\,) = r^2k = r^2w_1.$$

If $w_1 = r-1$, then $|N_G(Q)| + |M| = rw_1 + r^2w_1 = r(r-1) + r^2(r-1) = r(r^2-1) = |G|$. Since $N_G(Q) \cap M = \emptyset$, we have the desired result ($(a^2z+b)\left(\dfrac{-1}{z}\right)(z+d) = \dfrac{bz+(d-a^2)}{z+d}$ never fixes ∞). The other case is analogous. $\square$

Now let $1 \neq z+c \in Q$. By the lemma, $\left(\dfrac{-1}{z}\right)^{-1}(z+c)\left(\dfrac{-1}{z}\right) = (a^2z+b)\left(\dfrac{-1}{z}\right)(z+d)$ for some $a \in (\mathbb{F}_r)^\times$, $b,d \in \mathbb{F}_r$. The corresponding matrix equation is

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix}$$
$$\Longrightarrow \begin{pmatrix} 1 & 0 \\ -c & 1 \end{pmatrix} = \begin{pmatrix} \dfrac{b}{a} & -a+\dfrac{bd}{a} \\ \dfrac{1}{a} & \dfrac{d}{a} \end{pmatrix}.$$

Consequently, $c = \pm\dfrac{1}{a} \in (\mathbb{F}_r)^\times$ and Q is contained in (hence equal to since both have order r) $\{\, z+b \mid b \in \mathbb{F}_r \,\}$. $\square$

Lemma 4.14.

i) *If* $g \in PGL_2(\mathbb{F})$ *commutes with both* $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ *and* $\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right)$ *where* $t \neq 0$, *then* $g = 1$.

ii) *If* $g \in PGL_2(\mathbb{F})$ *commutes with both* $\left(\begin{smallmatrix} w & 0 \\ 0 & w^{-1} \end{smallmatrix}\right) \in PGL_2(\mathbb{F})$ *where* $w^4 \neq 1$ *and a matrix of the form* $\left(\begin{smallmatrix} x & \beta \\ \frac{y}{\beta} & -x \end{smallmatrix}\right)$ *where* $x, y, \beta \in \mathbb{F}^\times$, *then* $g = 1$.

iii) *If* $g \in U$ *commutes with both* $\left(\begin{smallmatrix} w & 0 \\ 0 & \overline{w} \end{smallmatrix}\right) \in U$ *where* $w\overline{w} = 1, w^2 \neq 1$ *and a matrix in* U *of the form* $\left(\begin{smallmatrix} y & z \\ -\overline{z} & -y \end{smallmatrix}\right)$ *where* $y \neq 0, z \neq 0$, *then* $g = 1$.

Proof: Let $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ where $ad - bc \neq 0$.

i) Since g commutes with $z + t$, g must fix ∞. Thus $c = 0$ and we may assume $d = 1$.

For $\lambda \in \mathbb{F}^\times$,

$$\begin{aligned} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} &= \lambda \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \\ \Longrightarrow \quad \begin{pmatrix} b & -a \\ 1 & 0 \end{pmatrix} &= \begin{pmatrix} 0 & -\lambda \\ \lambda a & \lambda b \end{pmatrix} \end{aligned}$$

Consequently, $b = 0, \lambda a = 1$ and $a = \lambda$. Therefore, $a^2 = 1$ and $g(z) = \pm z$. But $-z \circ (z + t) = -(z + t) = -z - t$ while $(z + t) \circ (-z) = -z + t$. Hence, $g = 1$.

ii) Since g commutes with $\begin{pmatrix} w & 0 \\ 0 & w^{-1} \end{pmatrix}$, we have

$$\begin{pmatrix} aw & \frac{b}{w} \\ cw & \frac{d}{w} \end{pmatrix} = \begin{pmatrix} \lambda aw & \lambda bw \\ \frac{\lambda c}{w} & \frac{\lambda d}{w} \end{pmatrix}$$

where $\lambda \neq 0$. Since $aw = \lambda aw$ and $\dfrac{d}{w} = \dfrac{\lambda d}{w}$, $a = d = 0$ or $\lambda = 1$. If $a = d = 0$, then $b \neq 0, c \neq 0$ since $ad - bc \neq 0$. Since $\dfrac{b}{w} = \lambda bw$ and $cw = \dfrac{\lambda c}{w}$, we have $\lambda = w^2 = \dfrac{1}{\lambda}$. Hence, $\lambda^2 = 1$ and $w^2 = \pm 1$. This is a contradiction since $w^4 \neq 1$. Thus, $a \neq 0$ or $d \neq 0$. In either case, it follows that $\lambda = 1$.

If $b \neq 0$ or $c \neq 0$, then we again get the contradiction that $w^2 = 1$. Hence, $g = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ with $a \neq 0$ or $b \neq 0$.

Since g commutes with $\begin{pmatrix} x & \beta \\ \frac{y}{\beta} & -x \end{pmatrix}$, we have

$$\begin{pmatrix} ax & a\beta \\ \frac{dy}{\beta} & -dx \end{pmatrix} = \begin{pmatrix} \mu ax & \mu\beta d \\ \frac{\mu ay}{\beta} & -\mu xd \end{pmatrix}$$

where $\mu \neq 0$. Since $x \neq 0$, we have $a = \mu a$ and $d = \mu d$. Since a and d are not both zero, $\mu = 1$. Since $\beta \neq 0$, the equation $a\beta = \mu\beta d$ thus gives $a = d$ so that g is the identity.

iii) Since $g \in U$, we have $d = -\overline{a}$ and $c = -\overline{b}$. Since g commutes with $\begin{pmatrix} w & 0 \\ 0 & \overline{w} \end{pmatrix}$, we have

$$\begin{pmatrix} aw & b\overline{w} \\ -\overline{b}w & -\overline{a}\overline{w} \end{pmatrix} = \begin{pmatrix} \lambda aw & \lambda bw \\ -\lambda\overline{b}\overline{w} & -\lambda\overline{a}\overline{w} \end{pmatrix}$$

for some $\lambda \neq 0$. If $b \neq 0$, then $\lambda w = \overline{w}$. Write $w = u + \alpha v$ where $u, v \in \mathbb{F}$. Then $\lambda u + \lambda\alpha v = u - \alpha v$. Consequently, $\lambda v = -v$ and $v = 0$. This implies that $w = u \in \mathbb{F}$, contradicting that $w^2 \neq 1$ (since $w\overline{w} = 1$). Hence, $b = 0$. It follows from the equations $b\overline{b} - a\overline{a} \neq 0$ and $a = \lambda a$ that $a \neq 0$ and $\lambda = 1$. Thus, g is of the form $\begin{pmatrix} a & 0 \\ 0 & \overline{a} \end{pmatrix}$.

Since g commutes with $\begin{pmatrix} y & z \\ -\overline{z} & -y \end{pmatrix}$,

$$\begin{pmatrix} ay & az \\ -\overline{a}\overline{z} & -\overline{a}y \end{pmatrix} = \begin{pmatrix} \mu ay & \mu\overline{a}z \\ -\mu a\overline{z} & -\mu\overline{a}y \end{pmatrix}$$

where $\mu \neq 0$. Since y and z are both nonzero, the equations $ay = \mu ay$ and $az = \mu\overline{a}z$ give that $\mu = 1$ and $\overline{a} = a$. Hence, $g = 1$. $\square$

Lemma 4.15. *Let* $1 \neq g = [A] \in PSL_2(\mathbb{F})$.

i) $|g| = 2$ *if and only if* $tr(A) = 0$.

ii) *If* $p > 3$, $|g| = 3$ *if and only if* $tr(A) = \pm 1$.

iii) $|g| = 4$ *if and only if* $tr^2(A) = 2$.

iv) *If* $p \neq 5$, $|g| = 5$ *if and only if* $tr^2(A) \pm tr(A) - 1 = 0$.

Proof: Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $ad - bc = 1$.

The characteristic polynomial $\chi_A(\lambda)$ of A is $\lambda^2 - \mathrm{tr}(A)\lambda + 1$. The eigenvalues of A are therefore $x, \dfrac{1}{x}$ where $x + \dfrac{1}{x} = \mathrm{tr}(A)$ (and $x \neq 0$).

The eigenvalues of A are distinct if and only if $\mathrm{tr}^2(A) \neq 4$ which happens if and only if $1 \neq g$ is not parabolic. Since in all cases of the lemma we are assuming A is not parabolic, A is conjugate to $D = \begin{pmatrix} x & 0 \\ 0 & \frac{1}{x} \end{pmatrix}$ and $|g| = |\,[D]\,|$. Moreover, $D^n = \pm I$ if and only if $x^n = \pm 1$.

Consequently, $|g| = 2 \iff x^2 = -1$, $|g| = 3 \iff x^3 = \pm 1$, $|g| = 4 \iff x^4 = -1$, $|g| = 5 \iff x^5 = \pm 1$ ($x^2 = 1 \implies g = 1$, $x^4 = 1 \implies 1 \leq |g| \leq 2$).

i) $\mathrm{tr}(A) = x + \dfrac{1}{x} = \dfrac{x^2+1}{x} = 0 \iff x^2 = -1$.

ii) $\dfrac{x^2+1}{x} = \pm 1 \iff x^2 + 1 = \pm x \iff x^2 \mp x + 1 = 0$. Since $x \neq \pm 1$, $x^2 \mp x + 1 = 0 \iff x^3 \pm 1 = (x \pm 1)(x^2 \mp x + 1) = 0 \iff x^3 = \mp 1$.

iii) $\left(x + \dfrac{1}{x}\right)^2 = 2 \iff x^2 + \dfrac{1}{x^2} + 2 = 2 \iff x^2 + \dfrac{1}{x^2} = 0 \iff \dfrac{x^4+1}{x^2} = 0 \iff x^4 = -1$.

iv) $\left(x + \dfrac{1}{x}\right)^2 + \left(x + \dfrac{1}{x}\right) - 1 = 0 \iff x^4 + x^3 + x^2 + x + 1 = 0 \iff x^5 - 1 =$

$(x-1)(x^4+x^3+x^2+x+1) \ = 0.$

Similarly, $\left(x+\dfrac{1}{x}\right)^2 - \left(x+\dfrac{1}{x}\right) - 1 = 0 \iff x^5+1 \ = \ (x+1)(x^4-x^3+x^2-x+1) \ = 0.$ □

Definition: Given $1 \neq g_1, g_2, g_3 \in PSL_2(q)$, let $m_i \ = |g_i|$. $X(m_1, m_2, m_3) := \{\ (\alpha, \beta, \gamma) \mid \gamma = (\alpha\beta)^{-1}, |\alpha| = m_1, |\beta| = m_2, |\gamma| = m_3\ \}$.

$PGL_2(q)$ acts on $X(m_1, m_2, m_3)$ by conjugation.

Lemma 4.16. *$PGL_2(q)$ acts freely and transitively on $X(2,p,3)$.*

Proof: We first choose an element g in $PSL_2(q)$ of order 2. Any element h of order p is parabolic. If h shares a fixed point with g, then g and h generate a dihedral group (and thus $|gh| = 2$). Using the fact that $PGL_2(q)$ acts triply transitively on $\widehat{\mathbb{F}_q}$ if g is hyperbolic and the fact that $PGL_2(q)$ acts transitively on $(\mathbb{F}_{q^2} - \mathbb{F}_q) \times \mathbb{F}_q$ if g is elliptic, we may assume $g(z) \ = \ \dfrac{-1}{z}$ and $h(z) \ = \ z+b$ (by conjugating the fixed points). But

$$A \ = \ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \ B \ = \ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \ AB \ = \ \begin{pmatrix} 0 & -1 \\ 1 & b \end{pmatrix}.$$

Therefore, $|gh| \ = \ 3 \iff \mathrm{tr}(AB) \ = \ b \ = \ \pm 1.$

Consequently, we can always conjugate g to $\dfrac{-1}{z}$ and h to $z \pm 1$. Since $-z$ sends $\dfrac{-1}{z}$ to itself and $z+1$ to $z-1$, $PGL_2(q)$ acts transitively on $X(2,p,3)$. It follows from Lemma 4.14(i) that the action is free. □

Theorem 4.17. *$PGL_2(q)$ acts freely and transitively on $X(2,3,3)$ and $X(2,3,4)$ and freely on $X(2,3,5)$. Moreover, the cardinality of $X(2,3,5)$ is $2q(q^2-1)$ when $q \neq 5^n$.*

Proof: We first consider the action of $PGL_2(q)$ on $X(2,3,5)$. When $q = 5^n$, the result follows from Lemma 4.16.

Case 1 $5 \mid (q-1)$

We first choose an element g of order 5. Since there are $\dfrac{q(q+1)}{2}$ choices for the fixed points of g and 4 choices for a generator of $< g > \cong \mathbb{Z}_5$, there are $4\left(\dfrac{q(q+1)}{2}\right) = 2q(q+1)$ choices for g. We may assume $g = \begin{pmatrix} \rho^\lambda & 0 \\ 0 & \rho^{-\lambda} \end{pmatrix}$ where $\lambda = \dfrac{q-1}{5}$.

We now compute the number of elements h such that $|h| = 2$, $|gh| = 3$. Now

$$h = \begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha \end{pmatrix}, \quad gh = \begin{pmatrix} \rho^\lambda \alpha & \rho^\lambda \beta \\ \rho^{-\lambda}\gamma & -\rho^{-\lambda}\alpha \end{pmatrix}$$

where $\det(h) = -\alpha^2 - \beta\gamma = 1$ and $\mathrm{tr}(gh) = \alpha(\rho^\lambda - \rho^{-\lambda}) = 1$. (If $\mathrm{tr}(A) = -1$, $\mathrm{tr}(-A) = 1$ and $\pm A$ represent the same matrix in $PSL_2(q)$.) Thus, $\alpha = (\rho^\lambda - \rho^{-\lambda})^{-1}$ and $\beta\gamma = -1 - (\rho^\lambda - \rho^{-\lambda})^{-2}$.

If $(\rho^\lambda - \rho^{-\lambda})^{-2} = -1$, then $w - 2 + w^{-1} = -1$ where $w = \rho^{2\lambda}$. Thus, $\frac{1}{w} = 1 - w$ and $w^2 - w + 1 = 0$. Since $w^3 + 1 = (w+1)(w^2 - w + 1)$, we have $w^3 = -1$ and $w^6 = 1$. But $< w > = < \rho^\lambda >$ and w has order 5. We thus get the contradiction that $1 = w^6 = ww^5 = w$. Consequently, $\beta\gamma \neq 0$ and $\gamma = \dfrac{-1 - (\rho^\lambda - \rho^{-\lambda})^{-2}}{\beta}$. Hence, there are $q-1$ choices for β (and therefore for h). Thus, $|X| = 2q(q+1)(q-1) = 2q(q^2-1)$.

Case 2 $5 \mid (q+1)$

Since elements of order 5 are elliptic, there are $4\left(\dfrac{q(q-1)}{2}\right) = 2q(q-1)$ choices for such a g. Working in the disk model, we may assume the fixed points of g are 0 and ∞. Thus, $g = \begin{pmatrix} x^m & 0 \\ 0 & \overline{x}^m \end{pmatrix}$ where $m = \dfrac{q+1}{5}$.

If $|h| = 2$ and $|gh| = 3$, then

$$h = \begin{pmatrix} y & z \\ -\overline{z} & -y \end{pmatrix}, \quad gh = \begin{pmatrix} yx^m & zx^m \\ -\overline{z}\overline{x}^m & -y\overline{x}^m \end{pmatrix}$$

where $\det(g) = (x\overline{x})^m = 1 = -y^2 + z\overline{z} = \det(h)$ and $\mathrm{tr}(gh) = y(x^m - \overline{x}^m) = 1$. Therefore, $y = (x^m - \overline{x}^m)^{-1}$ is determined. Moreover,

$$|z|^2 = z\overline{z} = 1 + y^2 = 1 + (x^m - \overline{x}^m)^{-2} \neq 0$$

(since $|x^m| = 5$). Since the norm map $N : \mathbb{E}^\times \longrightarrow \mathbb{F}^\times$ is surjective with kernel $\mathbb{S}$, there are $q+1$ elements z with $|z|^2 = 1 + (x^m - \overline{x}^m)^{-2}$. Thus, there are $q+1$ choices for h and $|X| = 2q(q^2-1)$.

In either case, we therefore have $|\ X(2,3,5)\ |$ is $2q(q^2-1)$ when $q \neq 5^n$. The fact that the action is free follows from Lemma 4.14 (and the proofs of cases 1 and 2 above).

If $q = 3^n$, $PGL_2(q)$ acts freely and transitively on $X(2,3,3)$ by Lemma 4.16. Let X be either $X(2,3,3)$ when $q \neq 3^n$ or $X(2,3,4)$. The arguments given in cases 1 and 2 above show that $PGL_2(q)$ acts freely on X (using Lemma 4.14) and $|X| = q(q^2-1)$. (Define $\lambda = \dfrac{q \pm 1}{3}, \dfrac{q \pm 1}{4}$ respectively and note that there are $q(q+1)$ choices for g since $\mathbb{Z}_3$ and $\mathbb{Z}_4$ each have only two generators.) Since $PGL_2(q)$ acts freely on $|X|$ and $|PGL_2(q)| = |X|$, it follows that the action is transitive. $\square$

Corollary 4.18. *Assume q is odd.*

i) $PSL_2(q)$ *contains a tetrahedral group.*

ii) *If $PSL_2(q)$ contains an element of order four, then it contains an octahedral group.*

iii) *If $PSL_2(q)$ contains an element of order five, then it contains an icosahedral group.*

Proof: The result follows from the proofs of Lemma 4.16 and Theorem 4.17. $\square$

Theorem 4.19. *Let $q = p^n$. There exists a subgroup of $PSL_2(q)$ isomorphic to*

i) $PSL_2(p^m)$ *if and only if* $m \mid n$.

ii) $PGL_2(p^m)$ *if and only if* $2m \mid n$ *when q is odd.*

iii) *a tetrahedral group except when* $q = 2^n$, n *odd.*

iv) *an octahedral group if and only if* $q \equiv \pm 1 \ (mod\ 8)$.

v) *an icosahedral group if and only if* $q(q^2-1) \equiv 0 \ (mod\ 5)$.

Proof: i) and ii) If $m \mid n$, then $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ and thus $PSL_2(p^m) \subseteq PSL_(p^n)$. Since $2m \mid n$, $PSL_2(p^{2m}) \subseteq PSL_2(p^n)$ by the above. Since $\mathbb{F}^\times \subseteq \mathbb{E}_+$, $PGL_2(\mathbb{F}) \subseteq PSL_2(\mathbb{E})$. Analogously, $PGL_2(p^m) \subseteq PSL_2(p^{2m})$. Therefore,

$$PGL_2(p^m) \subseteq PSL_2(p^{2m}) \subseteq PSL_2(p^n).$$

Conversely, if $PSL_2(p^n)$ contains a subgroup isomorphic to $PSL_2(p^m)$, it follows from the proof of Case 6A of Theorem 4.13 that $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$. Thus $\mathbb{F}_{p^n}$ is a vector space over $\mathbb{F}_{p^m}$ of dimension d. Consequently, $p^n = |\mathbb{F}_{p^n}| = (p^m)^d = p^{dm}$. Hence, $n = dm$ and $m \mid n$.

If $PSL_2(p^n)$ contains a subgroup isomorphic to $PGL_2(p^m)$ when p^n is odd, then $p^m(p^{2m}-1)$ divides $\dfrac{p^n(p^{2n}-1)}{2}$. Since $PSL_2(p^m) \subseteq PGL_2(p^m) \subseteq PSL_2(p^n)$, m divides n. Let $k > 0$ and consider the ring $R = \mathbb{Z}/2^k\mathbb{Z}$. Then

$$2^k \mid p^m \pm 1 \iff p^m \equiv \mp 1 (\text{mod } 2^k) \implies (p^m)^{2\ell+1} \equiv \mp 1 \ (\text{mod } 2^k).$$

Define $g_{2\ell+1} : R^\times \longrightarrow R^\times$ by $g_{2\ell+1}(x) = x^{2\ell+1}$ where $R^\times$ denotes the units of R. Clearly, $g_{2\ell+1}$ is a homomorphism since $R^\times$ is a multiplicative group. If $1 \neq x \in \ker(g_{2\ell+1})$, then $x^{2\ell+1} = 1$ and thus the order of x divides $2\ell+1$ and is odd. Since $R^\times$ consists of the equivalence classes of the odd integers, $|R^\times| = 2^{k-1}$. Thus, the order of x is even, giving a contradiction. Hence $\ker(g_{2\ell+1} = \{1\}$ and $g_{2\ell+1}$ is an automorphism of $R^\times$. Consequently, if $(p^m)^{2\ell+1} = \pm 1$ in $R^\times$, then

$$p^m = (g_{2\ell+1})^{-1}(g_{2\ell+1}(p^m)) = (g_{2\ell+1})^{-1}((p^m)^{2\ell+1}) = (g_{2\ell+1})^{-1}(\pm 1) = \pm 1 \text{ in } R^\times$$

(since $g_{2\ell+1}$ fixes ± 1). Hence, $(p^m)^{2\ell+1} \equiv \mp 1 \ (\text{mod } 2^k) \implies p^m \equiv \mp 1 (\text{mod } 2^k)$. Consequently, $2^k \mid p^m \pm 1 \iff 2^k \mid (p^{m(2\ell+1)} \pm 1)$. Hence, $p^m(p^{2m}-1)$ does not divide $\dfrac{p^{m(2\ell+1)}(p^{2m(2\ell+1)}-1)}{2}$. Therefore, $n = md$ where d is even and $2m$ divides n.

iii) If $p \neq 2$, then there exists a $g \in PSL_2(q)$ such that $\left\langle g(z), \dfrac{-1}{z} \right\rangle = \text{Alt}(4)$ by Cor. 4.18. If $p = 2^n$ with n even, then $\text{Alt}(4) \leq \text{Alt}(5) \cong PSL_2(2^2) \leq PSL_2(2^n)$.

Conversely, if $\mathrm{Alt}(4) \leq PSL_2(2^n)$, then an analysis of the proof of Theorem 4.13 shows that $\mathrm{Alt}(4) = QA_{0\infty}$. Now there is an element g of order 3 in Alt(4), hence in $A_{0\infty}$. Thus, g is hyperbolic and 3 divides $2^n - 1$. Consequently, n is even.

iv) If $\mathrm{Symm}(4) \leq PSL_2(q)$, then 8 divides $\mid PSL_2(q) \mid$ since the Sylow 2-subgroups of Symm(4) are dihedral of order 8. Since the Sylow p-subgroups of Symm(4) are conjugate to Q and thus abelian, $p \neq 2$. Thus, $8 \mid \dfrac{q(q^2-1)}{2} \implies 8 \mid \dfrac{q^2-1}{2}$ since q is odd $\implies 8 \mid (q \pm 1)$ since either $\dfrac{q+1}{2}$ or $\dfrac{q-1}{2}$ is odd.

Conversely, if $q \equiv \pm 1 \pmod 8$ then q is odd and there is an $h \in PSL_2(q)$ with $\left\langle h(z), \dfrac{-1}{z} \right\rangle = \mathrm{Symm}(4)$ by Corollary 4.18.

v) If $\mathrm{Alt}(5) \leq PSL_2(q)$, then 5 divides $\mid PSL_2(q) \mid$ and thus $5 \mid q(q^2-1)$.

If $q(q^2-1) \equiv 0 \pmod 5$ then 5 divides the order of $PSL_2(q)$. If q is odd, then there exists a $k \in PSL_2(q)$ with $\left\langle k(z), \dfrac{-1}{z} \right\rangle = \mathrm{Alt}(5)$ by Corollary 4.18. If q is even, then 5 divides $2^{2n}-1$ and therefore n must be even. Consequently, $\mathrm{Alt}(5) \cong PSL_2(4) \subseteq PSL_2(2^n)$. □

Lemma 4.20.

i) *Let $\beta \neq \gamma \in Alt(4)$ such that $|\beta| = |\gamma| = 3$. If $|\beta\gamma| = 3$, then $|\beta\gamma^{-1}| = 2$.*

ii) *If $Alt(4) \triangleleft G \leq PGL_2(q)$, $|G| = 24$ and G acts freely on $X(2,3,3) \cap Alt(4)$, then $G \cong Symm(4)$.*

Proof: i) Without loss of generality, we may assume $\beta = (123)$ and $\gamma =$

(243). Then $\beta\gamma = (123)(243) = (124)$ but $\beta\gamma^{-1} = (123)(234) = (12)(34)$ has order two.

ii) Since $\text{Alt}(4) \triangleleft G$, G acts by conjugation on the Sylow 3-subgroups of $\text{Alt}(4)$ giving a homomorphism $\phi : G \longrightarrow \text{Symm}(4)$. Since $|\text{Symm}(4)| = 24 = |G|$, it suffices to show that ϕ is 1-1. Suppose $\{1\} \neq k \in \ker(\phi)$. I.e., every Sylow 3-subgroup of $\text{Alt}(4)$ is invariant under conjugation by k.

Let $(\alpha, \beta, \gamma) \in W(2,3,3)$. Since $k^{-1}\beta k \in \{\beta, \beta^{-1}\}$ and $k^{-1}\gamma k \in \{\gamma, \gamma^{-1}\}$, we must have $k^{-1}\beta k = \beta^{-1}$ and $k^{-1}\gamma k = \gamma^{-1}$. (Since G acts freely on $W(2,3,3)$, $k^{-1}\beta k = \beta$ and $k^{-1}\gamma k = \gamma$ is impossible. The other two possibilities are ruled out by i) above.) Since $\alpha\beta\gamma = 1$, $\alpha = (\beta\gamma)^{-1} = \gamma^{-1}\beta^{-1}$. Now $(\alpha, \beta\gamma^{-1}, \gamma^2)$ is in $W(2,3,3)$ also ($|\beta\gamma| = 2 \implies |\beta\gamma^{-1}| = 3$ by part i)). By the same reasoning as above, $k^{-1}(\beta\gamma^{-1})k = (\beta\gamma^{-1})^{-1} = \gamma\beta^{-1}$ and $k^{-1}\gamma^2 k = (\gamma^2)^{-1} = \gamma$. But $(k^{-1}\alpha k)\beta^{-1}\gamma^{-1} = 1$ which implies $k^{-1}\alpha k = \gamma\beta$. Consequently, $(\gamma\beta)(\gamma\beta^{-1})\gamma = 1$ thus implying that $\gamma\beta\gamma = \gamma^{-1}\beta$ and $\beta\gamma = \gamma^{-2}\beta = \gamma\beta$. This is a contradiction since $< \alpha, \beta, \gamma >$ is not abelian. Hence, $\ker(\phi) = \{1\}$. $\square$

Theorem 4.21. *$PSL_2(q)$ contains the following conjugacy classes of subgroups where $g = |\, PSL_2(q) \,|$ and $q = p^n$ is odd.*

i) *There is one conjugacy class containing $\dfrac{q(q-1)}{2}$ $\mathbb{Z}_k$'s for each $k > 1$ dividing $\dfrac{q+1}{2}$ and one conjugacy class containing $\dfrac{q(q+1)}{2}$ $\mathbb{Z}_k$'s for each $k > 1$ dividing $\dfrac{q-1}{2}$.*

ii) *There are $\dfrac{g}{2k}$ D_k's for each $k > 2$ dividing $\dfrac{q \pm 1}{2}$ which form two* *conjugacy classes when* $\frac{q \pm 1}{2}$ *is even and one otherwise. There are* $\frac{g}{12}$ D_2*'s which form two conjugacy classes when* $q \equiv \pm 1 \pmod 8$ *and one otherwise.*

iii) *There are* $\frac{g}{12}$ *tetrahedral groups forming two conjugacy classes when* $q \equiv \pm 1 \pmod 8$ *and one otherwise. If* $q \equiv \pm 1 \pmod 8$, *there are two conjugacy classes of octahedral groups, each containing* $\frac{g}{24}$ *copies. There are* $\frac{g}{30}$ *icosahedral groups which form two conjugacy classes if* $q \equiv \pm 1 \pmod 5$. *If* $q = 5^n$ *there are* $\frac{g}{60}$ *icosahedral subgroups forming one conjugacy class when* n *is odd and two when* n *is even.*

Proof: Let $\mathbb{F} = \mathbb{F}_q$.

i) For each pair $x \neq y \in \widehat{\mathbb{F}}$, $< g >$ is conjugate to $\mathbb{F}_+ z \cong \mathbb{Z}_{\frac{q+1}{2}}$ where g is a hyperbolic element fixing x and y. Thus, there are $\frac{(q+1)q}{2}$ conjugate copies of $\mathbb{Z}_{\frac{q+1}{2}}$. Each such $\mathbb{Z}_{\frac{q+1}{2}}$ contains a unique cyclic subgroup of order k for each $k > 1$ dividing $\frac{q-1}{2}$.

Similarly, there are $\frac{(q^2-q)}{2}$ conjugate copies of $\mathbb{Z}_{\frac{q-1}{2}} \cong PSL_2(q)_\gamma$, one for each $\gamma \in \mathbb{E} - \mathbb{F}$.

ii) Each $\mathbb{Z}_{\frac{q-1}{2}} \cong PSL_2(q)_{\{x,y\}}$ determines a unique

$$D_{\frac{q-1}{2}} \cong N(PSL_2(q)_{\{x,y\}}) = \left\langle PSL_2(q)_{\{x,y\}}, g_{\{x,y\}} \right\rangle$$

where $g_{\{x,y\}}$ is an element of order two interchanging x and y. Thus, there are $\frac{q(q+1)}{2}$ conjugate copies of $D_{\frac{q-1}{2}}$.

For $m > 2$ dividing $\frac{q-1}{2}$, there are $\frac{q-1}{2m}$ copies of D_m within each

$D_{\frac{q-1}{2}}$ and thus $\left(\frac{q(q+1)}{2}\right)\left(\frac{q-1}{2m}\right) = \frac{g}{2m}$ distinct copies of D_m. (No D_m is contained in more than one $D_{\frac{q-1}{2}}$ since there is a unique subgroup $\mathbb{Z}_m$ contained in D_m.) Moreover, there are two conjugacy classes of D_m within $D_{\frac{q-1}{2}}$ if $\frac{q-1}{2m}$ is even and one otherwise. (The normalizer of D_m in D_n is D_{2m} when $\frac{n}{m}$ is even and D_m is self-normalizing in D_n otherwise.)

Similarly, we get the result for $D_{\frac{q+1}{2}} \cong N\left(PSL_2(q)_{\{\alpha,\overline{\alpha}\}}\right)$ and its dihedral subgroups of order larger than 4.

Assume 2 divides $\frac{q-1}{2}$. Now there are $\frac{q-1}{4}$ D_2's per $D_{\frac{q-1}{2}}$. Say that $D_2 = \{ 1, x, y, z \}$. Since the fixed point sets of x, y and z are distinct, D_2 is contained in exactly three copies of $D_{\frac{q-1}{2}}$. Thus, there are

$$\frac{\left[\frac{q(q+1)}{2}\right]\left[\frac{q-1}{4}\right]}{3} = \frac{g}{12}$$

distinct D_2's. Now $N(D_2) = D_2 \rtimes \mathbb{Z}_3 \cong \mathrm{Alt}(4)$ unless Symm(4) exists, in which case $N(D_2) \cong$ Symm(4). Hence, there are two conjugacy classes of D_2 when $q \equiv \pm 1 \pmod 8$ and one otherwise.

The case when 2 divides $\frac{q+1}{2}$ is analogous.

iii) Assume $q \equiv \pm 1 \pmod 5$ and fix one copy of $\mathrm{Alt}(5) \leq PSL_2(q)$. Let $W(2,3,5)$ be the subset of $X(2,3,5)$ with $\alpha, \beta \in \mathrm{Alt}(5)$.

Note that $G = \mathrm{Symm}(5)$ acts by conjugation on $W(2,3,5)$. Let (α,β,γ) and (α',β',γ') be in $W(2,3,5)$. Now $1 \neq g \in G_{(\alpha,\beta,\gamma)} \implies g^{-1}\alpha g = \alpha$, $g^{-1}\beta g = \beta$, and $g^{-1}\gamma g = \gamma$ which implies g is in the centralizer of $< \alpha,\beta,\gamma > =$ Alt(5). Since the centralizer of Alt(5) is trivial, so is $G_{(\alpha,\beta,\gamma)}$.

Define $h : \mathrm{Alt}(5) \longrightarrow \mathrm{Alt}(5)$ by $h(\alpha) = \alpha'$, $h(\beta) = \beta'$, $h(\gamma) = \gamma'$. Since h takes a set of generators of Alt(5) to a set of generators of Alt(5) and preserves the relations, h is a group homomorphism (hence an automorphism) of Alt(5). But every automorphism of Alt(5) acts by conjugation. Thus, there exists a $g \in \mathrm{Symm}(5)$ such that $\alpha' = h(\alpha) = g^{-1}\alpha g$, $\beta' = h(\beta) = g^{-1}\beta g$, $\gamma' = h(\gamma) = g^{-1}\gamma g$. I.e., Symm(5) acts transitively on $W(2,3,5)$. Consequently,

$$|W(2,3,5)| = |G_x| = \frac{|\mathrm{Symm}(5)|}{|G_x|} = 120$$

where G_x denotes the stabilizer of $x = (\alpha, \beta, \gamma)$.

Analogously, we can prove that Symm(4) acts freely and transitively on $W(2,3,3)$ and $W(2,3,4)$ and thus $|W(2,3,3)| = 24 = |W(2,3,4)|$.

The number of distinct icosahedral subgroups of $PSL_2(q)$ is thus

$$\frac{|X(2,3,5)|}{|W(2,3,5)|} = \begin{cases} \dfrac{q(q^2-1)}{120} = \dfrac{g}{60} & \text{if } q = 5^n, \\ \dfrac{2q(q^2-1)}{120} = \dfrac{g}{30} & \text{otherwise.} \end{cases}$$

The number of distinct tetrahedral and octahedral subgroups of $PSL_2(q)$ is

$$\frac{|X(2,3,3)|}{|W(2,3,3)|} = \frac{g}{12} = \frac{|X(2,3,4)|}{|W(2,3,4)|}.$$

Since $|W(2,3,4)| = 24$ and $N_{PGL_2(q)}(\mathrm{Symm}(4))$ preserves $W(2,3,4)$, $|N_{PGL_2(q)}(\mathrm{Symm}(4))| \leq 24$. But $\mathrm{Symm}(4) \leq N_{PGL_2(q)}(\mathrm{Symm}(4))$ so that $N_{PGL_2(q)}(\mathrm{Symm}(4)) = \mathrm{Symm}(4)$. Consequently, Symm(4) is also self-normalizing in $PSL_2(q)$. Since each conjugacy class contains

$\frac{g}{|N_{PGL_2(q)}(\mathrm{Symm}(4))|} = \frac{g}{24}$ subgroups, there are two conjugacy classes of octahedral groups.

Similarly, $|N_{PGL_2(q)}(\mathrm{Alt}(4))| \leq 24$ since $N_{PGL_2(q)}(\mathrm{Alt}(4))$ preserves $W(2,3,3)$ which has cardinality 24. Since $\mathrm{Alt}(4) \leq N_{PGL_2(q)}(\mathrm{Alt}(4))$, we have that $12 \leq |N_{PGL_2(q)}(\mathrm{Alt}(4))| \leq 24$ which implies that either Alt(4) is self-normalizing in $PGL_2(q)$ or Alt(4) has index two in its normalizer in $PGL_2(q)$. In the latter case, $N_{PGL_2(q)}(\mathrm{Alt}(4)) = \mathrm{Symm}(4)$ by Lemma 4.20. Consequently, the normalizer of Alt(4) in $PSL_2(q) \cong \mathrm{Symm}(4)$ when $\mathrm{Symm}(4) \leq PSL_2(q)$ and is Alt(4) otherwise.

Let $N := N_{PGL_2(q)}(\mathrm{Alt}(5))$. Since N preserves $W(2,3,5)$ which has cardinality 120 and $\mathrm{Alt}(5) \subseteq N$, we know that $60 \leq |N| \leq 120$.

Assume $p \neq 5$. Given an element $g \in \mathrm{Alt}(5)$ of order 5, we may conjugate so that the fixed points of g are 0 and ∞ and thus

$$\mathbb{Z}_5 \cong \left\langle 1,\ \lambda^2 z,\ \lambda^4 z,\ \frac{z}{\lambda^2},\ \frac{z}{\lambda^4} \right\rangle.$$

We can conjugate $\lambda^2 z$ to $\frac{z}{\lambda^2}$ (and $\lambda^2 z$ to $\frac{z}{\lambda^4}$) by an element of order two which interchanges 0 and ∞. Since the trace of a matrix is invariant under conjugation and

$$\operatorname{tr}\begin{pmatrix} \lambda & 0 \\ 0 & \frac{1}{\lambda} \end{pmatrix} = \lambda + \frac{1}{\lambda} \neq \lambda^2 + \frac{1}{\lambda^2} = \operatorname{tr}\begin{pmatrix} \lambda^2 & 0 \\ 0 & \frac{1}{\lambda^2} \end{pmatrix},$$

$\lambda^2 z$ and $\lambda^4 z$ are not conjugate. Thus, there are exactly two $PGL_2(q)$ conjugacy classes of elements of order 5 in Alt(5).

Fix an element g of order 5 in Alt(5) and let W be the subset of $W(2,3,5)$

consisting of all (α,β,γ) with γ conjugate to g. Then $|W| = \dfrac{|W(2,3,5)|}{2}$. (There are 2 (not 4) choices for a generator of each $\mathbb{Z}_5$.) Since $N \leq PGL_2(q)$ acts freely on W, $|N| \leq 60$. Consequently, Alt(5) is also self-normalizing in $PSL_2(q)$ and there are thus two conjugacy classes of icosahedrals in $PSL_2(q)$.

Assume $q = 5^n$. We observe that in the proof of Lemma 4.16, we showed that given (α,β,γ) in $X(2,3,5)$ we can conjugate so that $< \alpha,\beta,\gamma > \cong \left\langle \dfrac{-1}{z}, z+1 \right\rangle = PSL_2(5)$. Thus, Alt(5) $= PSL_2(5) \triangleleft PGL_2(5)$ which implies that $PGL_2(5)$ is contained in (hence equal to) N. So

$$N_{PSL_2(5^n)}(PSL_2(5^n)) = \begin{cases} PSL_2(5^n) & \text{if} \quad n \ \text{ is odd,} \\ \\ PGL_2(5^n) & \text{if} \quad n \ \text{ is even.} \end{cases}$$

Hence, there are two conjugacy classes of icosahedrals when $q = 5^n$ and n is even and one when n is odd. $\square$

5. The Eichler Cohomology of $PSL_2(p)$.

Let $V_n(\mathbb{F})$ be the vector space of polynomials (in one variable) of degree at most n with coefficients in $\mathbb{F}$ and $H_n(\mathbb{F})$ the vector space of homogeneous polynomials (in two variables) of degree n with coefficients in $\mathbb{F}$.

Let $p(z,w) = a_n z^n + a_{n-1}z^{n-1}w + \cdots + a_0 w^n \in H_n(\mathbb{F})$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{F})$. Then $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} z \\ w \end{pmatrix} = \begin{pmatrix} az+bw \\ cz+dw \end{pmatrix}$.

$SL_2(\mathbb{F})$ acts on $H_n(\mathbb{F})$ via

$$(pg)(z,w) := a_n(az+bw)^n + a_{n-1}(az+bw)^{n-1}(cz+dw) + \cdots + a_0(cz+dw)^n.$$

Since $p(\lambda z, \lambda w) = \lambda^n p(z,w)$ for $\lambda \neq 0$, there is an induced action of $PSL_2(\mathbb{F})$ on $H_n(\mathbb{F})$ when n is even. Unfortunately, we see than an analog of this action for $PGL_2(\mathbb{F})$ is not so obvious.

Given $n = 2r-2$, $p \in V_n$ and $g \in PSL_2(\mathbb{F})$, define

$$(*) \qquad (pg)(z) = p(g(z))(g'(z))^{1-r}.$$

Consider the following diagram where the vertical maps are given by dehomogenizing the polynomials of $H_n(\mathbb{F})$ (setting $w=1$):

$$\begin{array}{ccc} H_n(\mathbb{F}) & \xrightarrow{g} & H_n(\mathbb{F}) \\ \downarrow & & \downarrow \\ P_n(\mathbb{F}) & \xrightarrow{g} & P_n(\mathbb{F}) \end{array}$$

This diagram commutes and the top map defines an action. Since the vertical maps are isomorphisms, (*) also defines an action of $PSL_2(\mathbb{F})$ on $V_n(\mathbb{F})$.

Let $G \leq PSL_2(\mathbb{F})$, n an even positive integer. We define the **n-cochains of G with coefficients in** $V_n(\mathbb{F})$ where $n \in \{0,1,2\}$ as follows:

$$C^0(G, V_n(\mathbb{F})) := V_n(\mathbb{F}),$$

$$C^1(G; V_n(\mathbb{F})) := \{ \, F : G \longrightarrow V_n(\mathbb{F}) \mid F(1) = 0 \, \},$$

$$C^2(G; V_n(\mathbb{F})) := \{ F : G \times G \longrightarrow V_n(\mathbb{F}) \mid \; F(g,1) = 0 = F(1,g) \, \}.$$

We have the following coboundary maps: If $p \in V_n(\mathbb{F}) = C^0(G; V_n(\mathbb{F}))$ and $g \in G$,

$$d_0{}^* : C^0(G; V_n(\mathbb{F})) \longrightarrow C^1(G; V_n(\mathbb{F})) \text{ via } d_0{}^*(p)(g) := pg - p$$

If $F \in C^1(G; V_n(\mathbb{F}))$ and $g, h \in G$,

$$d_1{}^* : C^1(G; V_n(\mathbb{F})) \longrightarrow C^2(G; V_n(\mathbb{F})) \text{ via } d_1{}^*(F)(g,h) := F(g)h - F(gh) + F(h)$$

Let

$$Z^1(G; V_n(\mathbb{F})) := \ker(d_1{}^*) \; = \{ \, F : G \longrightarrow V_n(\mathbb{F}) \mid F(1) = 0, F(gh) = F(g)h + F(h) \, \},$$

$$B^1(G; V_n(\mathbb{F})) := \mathrm{Im}(d_0{}^*) \; = \{ \, F : G \longrightarrow V_n(\mathbb{F}) \mid F(g) = pg - p \text{ for all } g \in G \, \}.$$

Elements of $Z^1(G; V_n(\mathbb{F}))$ (respectively $B^1(G; V_n(\mathbb{F}))$) are called **1-cocycles** (respectively **1-coboundaries**) **of G with $V_n(\mathbb{F})$ coefficients.** The **Eichler cohomology of G with $V_n(\mathbb{F})$ coefficients** is

$$H^1(G; V_n(\mathbb{F})) \; := \; Z^1(G; V_n(\mathbb{F})) / B^1(G; V_n(\mathbb{F})).$$

In other words, the Eichler cohomology of G is the first group cohomology of G (see [M],[Br]).

Given $g \in G$, let $\mathrm{Res}|^G_{<g>}$ denote the restriction map from $H^1(G; V_n(\mathbb{F}))$ to $H^1(< g >; V_n(\mathbb{F}))$.

The **parabolic 1-cocycles of G with $V_n(\mathbb{F})$ coefficients** is

$$PZ^1(G; V_n(\mathbb{F})) = \left\{ F \in Z^1(G; V_n(\mathbb{F})) \mid F \in \bigcap_{\substack{g \in G \\ g \text{parabolic}}} \ker\left(\mathrm{Res}|^G_{<g>}\right) \right\}.$$

I.e., a parabolic cocycle is a cocycle which is a coboundary when restricted to every parabolic element of G.

The **parabolic cohomology of G with $V_n(\mathbb{F})$ coefficients** is

$$PH^1(G; V_n(\mathbb{F})) = PZ^1(G; V_n(\mathbb{F}))/B^1(G; V_n(\mathbb{F})).$$

Let $g(z) = \dfrac{az+b}{cz+d} \in PSL_2(\mathbb{F})$ and $p(z) = rz^2 + sz + t \in V_2(\mathbb{F})$. Then $g'(z) = (cz+d)^{-2}$ and

$$\begin{aligned} (pg)(z) &= p(g(z))(g'(z))^{-1} = p(g(z))(cz+d)^2 \\ &= r(az+b)^2 + s(az+b)(cz+d) + t(cz+d)^2 \\ (**) \qquad &= (ra^2 + sac + tc^2)z^2 + (2rab + s(ad+bc) + 2tcd)z + (rb^2 + sbd + td^2). \end{aligned}$$

Let $V^G := \{ p \in V_2(\mathbb{F}) \mid pg = p \text{ for all } g \in G \}$ and let $V^g := V^{<g>}$.

Remark 5.1

i) If $g(z) = -\dfrac{1}{z}$ $(a = 0 = d, b = -1, c = 1)$, then $(pg)(z) = tz^2 - sz + r$ and $V^g = \{ rz^2 + r \mid r \in \mathbb{F} \}$.

ii) If $1 \neq g(z) = z + b$ $(a = 1 = d, c = 0)$, then $(pg)(z) = rz^2 + (2rb + s)z + (rb^2 + sb + t)$ and $V^g = \{ t \mid t \in \mathbb{F} \}$.

iii) If $g(z) = \lambda^2(z), \lambda^2 \neq 1$ $(a = \lambda, b = 0 = c, d = \lambda^{-1})$, then $(pg)(z) = r\lambda^2 z^2 + sz + t\lambda^{-2}$ and $V^g = \{ sz \mid s \in \mathbb{F} \}$.

iv) If $g(z) = \begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix}$ and $a \notin \{0,1\}, b \neq 0$, then $(pg)(z) = ra^2z^2 + (2rab + s)z + (rb^2 + sa^{-1}b + ta^{-2})$. If $p \in V^g$, then $2rab + s = s$ which implies that $r = 0$.

We also must have $sa^{-1}b + ta^{-2} = t$ or equivalently, $t(a^{-2} - 1) = -sa^{-1}b$. If $a = -1$, then we get $sb = 0 \implies s = 0$. Otherwise, $t = \dfrac{-sab}{1 - a^2} = \dfrac{abs}{a^2 - 1}$.

Therefore, $V^g = \{ t \mid t \in \mathbb{F} \}$ if $p = 3$ and $V^g = \{ sz + \dfrac{abs}{a^2 - 1} \mid s \in \mathbb{F} \}$ otherwise.

Note that every elliptic element of $PSL_2(q)$ is a hyperbolic element in $PSL_2(q^2)$. Consequently, every hyperbolic or elliptic element in $PSL_2(q)$ is conjugate to an element of the form $\lambda^2 z, \lambda \in (\mathbb{F}_{q^2})^{\times}$. Moreover, if $\mathbb{F} = \mathbb{F}_q$ and $\mathbb{E} = \mathbb{F}_{q^2}$,

$$\dim_{\mathbb{E}}(H^1(PSL_2(\mathbb{F}); V_n(\mathbb{F}) \otimes_{\mathbb{E}} \mathbb{E})) = \dim_{\mathbb{F}}(H^1(PSL_2(\mathbb{F}); V_n(\mathbb{F}))).$$

(Changing coefficients from $V_n(\mathbb{F})$ to $V_n(\mathbb{E})$ is equivalent to applying the exact functor $\otimes_{\mathbb{F}}\mathbb{E}$ to the cochain complex $\{C^k(G; V_n(\mathbb{F})), {d_k}^*\}$:

$$\cdots \longrightarrow C^k(G; V_n(\mathbb{F})) \xrightarrow{{d_k}^*} C^{k+1}(G; V_n(\mathbb{F})) \longrightarrow \cdots$$

$$\cdots \longrightarrow C^k(G; V_n(\mathbb{F})) \otimes_{\mathbb{F}} \mathbb{E} \xrightarrow{{d_k}^*} C^{n+1}(G; V_n(\mathbb{F})) \otimes_{\mathbb{F}} \mathbb{E} \longrightarrow \cdots.$$

The coboundary map ${d_k}^*$ of both chain complexes is given by the same matrix since $\mathbb{F} \subseteq \mathbb{E}$ and thus the dimension of cohomology will be the same no matter which chain complex we use.)

Remark 5.2 In particular, to find the dimension of $H^1(G; V_2(\mathbb{F})$ (or of $PH^1(G; V_2(\mathbb{F}))$ for any maximal nonprojective subgroup G of $PSL_2(q)$, it suffices to compute the dimensions of the cohomology of the following groups:

i) $< \lambda^2 z >$, $\lambda \in (\mathbb{F}_{q^2})^\times, \lambda^2 \neq 1$ (Cartan)

ii) $\langle \lambda^2 z, \frac{-1}{z} \mid (\frac{-1}{z} \circ \lambda^2 z)^2 = 1 \rangle, \lambda \in (\mathbb{F}_{q^2})^\times, \lambda^2 \neq 1$ (dihedral)

iii) $\langle z+1, \lambda^2 z \rangle, \lambda \in (\mathbb{F}_q)^\times, \lambda^2 \neq 1$ (Borel)

iv) a tetrahedral, octahedral, or icosahedral subgroup of $PSL_2(q)$.

In addition, we will compute the dimension of the cohomology of the following groups:

v) $< z+1 >$ (cyclic parabolic),

vi) $\{ z+b \mid b \in \mathbb{F}_q \}$ (full parabolic),

vii) $\langle \frac{-1}{z}, z+1 \rangle$ $(PSL_2(p))$.

We will therefore have computed the dimension of $H^1(G; V_2(\mathbb{F})$ (and $PH^1(G; V_2(\mathbb{F}))$ for any subgroup G of $PSL_2(p)$. For the remainder of this chapter, let $\mathbb{F} = \mathbb{F}_q$ where $q = p^n$ is odd, $\mathbb{E} = \mathbb{F}_{q^2}$, $V = V_2(\mathbb{F})$, and $G \leq PSL_2(\mathbb{F})$.

If G is an **exceptional** subgroup of $PSL_2(q)$ (i.e., a tetrahedral, octahedral or icosahedral subgroup), then we may assume $G = \left\langle A = \dfrac{-1}{z}, B = \begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix} \right\rangle$ where $a^2 - a + 1 = 0$ and $b = 1$ if G is tetrahedral, $b^2 = 2$ if G is octahedral, $b^2 - b - 1 = 0$ if G is icosahedral. (It follows from Lemma 4.15 that $|B| = 3$ and $|AB| \in \{3, 4, 5\}$ so that $< A, B >$ is an exceptional subgroup. We are also using the fact that every elliptic element of order $3, 4$, or 5 is hyperbolic or parabolic in $\mathbb{F}_{q^2}$ (so that a and b exist in $\mathbb{F}_{q^2}$).)

Remark 5.3: i) It follows from Remark 5.1 that $V^G = \{ t \mid t \in \mathbb{F} \}$ for the full parabolic subgroup and the cyclic subgroups listed above and that $V_G = \{0\}$ for all the others.

ii) Note that Remark 5.1 and i) above show that $p \in V^g$ for $g \in PSL_2(q)$ if and only if the fixed points of g are the roots of p (where p is thought of as a homogeneous polynomial). In particular, $V^G = \{0\}$ for every noncyclic subgroup G of $PSL_2(p)$.

We have

$$0 \longrightarrow C^0(G;V) \xrightarrow{d_0^*} C^1(G;V) \xrightarrow{d_1^*} C^2(G;V).$$

Since $C^0(G;V) = V$ is a vector space and $d_0{}^*$ is a linear map,

$$\dim(\mathrm{Im}(d_0)^*) \;=\; \dim(V) - \dim(\ker(d_0{}^*)) \;=\; 3 - \dim(\ker(d_0{}^*)).$$

Now $p \in \ker(d_0{}^*) \iff d_0{}^*(p) \equiv 0 \iff d_0{}^*(p)(g) = pg - p = 0$ for all $g \in G \iff p \in V^G$. Therefore, $\ker(d_0{}^*) = V^G$. Consequently, $B^1(G;V)$ has dimension 2 for the full parabolic and the cyclic subgroups on the list and dimension three for all the others.

Assume $F : G \longrightarrow V$ such that $F(1) = 0$ and $F(gh) = F(g)h + F(h)$. Then $0 = F(1) = F(gg^{-1}) = F(g)g^{-1} + F(g^{-1})$ and therefore $F(g^{-1}) = -F(g)g^{-1}$.

If $g(z) = \dfrac{-1}{z} \in G$, let $F(\dfrac{-1}{z}) = rz^2 + sz + t$. Since $g^2 = 1, g^{-1} = g$ and

$0 = F(1) = F(g)g + F(g) = (tz^2 - sz + r) + (rz^2 + sz + t) = (r+t)z^2 + (r+t)$.

Therefore, $t = -r$. Consequently,

$$\boxed{F\left(\frac{-1}{z}\right) = rz^2 + sz - r}\,. \tag{5–4}$$

If $1 \neq g(z) = z + b \in G$, let $F(g) = rz^2 + sz + t$. Since g is parabolic, $g^p = 1$. Therefore,

$$0 = F(1) = F(g^p) = F(gg^{p-1}) = F(g)g^{p-1} + F(g^{p-1}) \;=\; F(g)g^{p-1} + F(gg^{p-2})$$
$$= F(g)g^{p-1} + F(g)g^{p-2} + F(g^{p-2})$$
$$\vdots$$
$$= F(g)(g^{p-1} + g^{p-2} + \cdots + g + 1)$$

Since $\mathrm{char}(\mathbb{F}) = p$, $(1-g)^p = 1 - g^p = (1-g)(1 + g + \cdots + g^{p-1})$ and thus $(1-g)^{p-1} = 1 + g + g^2 + \cdots + g^{p-1}$. Therefore, $0 = F(g)(1-g)^{p-1}$.

For any $p(z) \in V$, $(pg)(z) = p(z+b)$ and $p(1-g)(z) = p(z) - (pg)(z) = p(z) - p(z+b)$ has degree one less than the degree of $(pg)(z)$. Thus, $p(1-g)(z)$ has degree at most one.

Since $p(1-g)^2 = [p(1-g)](1-g)$, $\deg(p(1-g)^2) \leq 0$. Consequently, $\deg(p(1-g)^k) = 0$ for $k \geq 3$. In particular, if $j(z) = F(g) \in V$, then $0 = j(1-g)^k = F(g)(1-g)^k$ for all $k \geq 3$. Thus, the equation "$0 = F(g)(1-g)^{p-1}$" is always true for $p - 1 \geq 3$ ($\iff$ $p \neq 3$) and $F(z+b)$ can be any element of V.

If $p = 3$, then $0 = F(g)(1-g)^2$ implies

$$\begin{aligned} 0 &= [F(g)(1-g)](1-g) \;=\; [F(g) - F(g)g](1-g) \\ &= [rz^2 + sz + t - r(z+b)^2 - s(z+b) - t](1-g) \;=\; [-(2rz + b^2r + sb)](1-g) \\ &= -(2rz + b^2r + sb) + 2r(z+b) + b^2r + sb \;=\; 2rb. \end{aligned}$$

Therefore, $r = 0$.

(5–5) $$\boxed{F(z+b) = sz + t \text{ if } p = 3, \quad F(z+b) = rz^2 + sz + t \text{ otherwise}}.$$

If $g(z) = \lambda^2 z \in G$ and $\lambda^2 \neq 1$, let $F(\lambda^2 z) = rz^2 + sz + t$. Assume g has order m. Then

$$0 = F(1) = F(g^m) = F(g)(1 + g + g^2 + \cdots + g^{m-1})$$
$$= F(g) + F(g)g + F(g)g^2 + \cdots + F(g)g^{m-1}.$$

Since $g^k(z) = \lambda^{2k}$, $F(g)g^k(z) = r\lambda^{2k}z^2 + sz + t\lambda^{-2k}$ by Remark 5.1. Therefore,

$$0 = (rz^2 + sz + t) \;+\; (r\lambda^2 z^2 + sz + t\lambda^{-2}) \;+\; \ldots \;+\; (r\lambda^{2(m-1)}z^2 + sz + t\lambda^{-2(m-1)})$$
$$= r(1 + \lambda^2 + \lambda^4 + \cdots + \lambda^{2(m-1)})z^2 \;+\; msz \;+\; t(1 + \lambda^{-2} + \lambda^{-4} + \cdots + \lambda^{-2(m-1)}).$$

Therefore, $0 \;=\; r\left(\dfrac{1-\lambda^{2m}}{1-\lambda^2}\right) z^2 \;+\; msz \;+\; t\left(\dfrac{1-\lambda^{-2m}}{1-\lambda^{-2}}\right)$. But $\lambda^{2m} = 1 = \lambda^{-2m}$ since g has order m. Therefore, $ms = 0$. Since $m < p$, we must have $s = 0$. Consequently,

(5–6) $$\boxed{F(\lambda^2 z) \;=\; rz^2 + t}.$$

We have shown that $\dim(Z^1(< z+1 >; V) = 2$ if $p = 3$ and 3 otherwise and that $\dim(Z^1(< \lambda^2 z >; V) = 2$. Consequently, $H^1(< z+1 >; V)$ is one dimensional if $p \neq 3$ and trivial for $p = 3$. Likewise, $H^1(< \lambda^2 z >; V)$ $(= PH^1(< \lambda^2 z >; V))$ is trivial. Since every element of $< z+1 >$ is parabolic, $PH^1(< z+1 >; V) = H^1(< z+1 >; V)$.

Remark 5.7 Suppose $F \in PZ^1(G; V)$. If G contains a parabolic element, then we may assume $g(z) = z + b \in G$. Then $F(z+b) = p(z+b) - p(z)$ for some $p \in V$. I.e., $F(z+b)$ has at most degree one.

Remark 5.8 Let $G = \{\, z+b \mid b \in \mathbb{F} \,\}$. We know that $\dim(B^1(G;V)) = 2$. Since G has n generators and $F(z+b)$ can be any element of V, $\dim(Z^1(G;V)) = n\dim(V) = 3n$. Therefore, $H^1(G;V)$ has dimension $3n-2$. If $F \in PZ^1(G;V)$, then $F(z+b) = sz+t$ for some $s,t \in \mathbb{F}$. Therefore, $PZ^1(G;V)$ has dimension $2n$ and $PH^1(G;V)$ has dimension $2n-2$.

Lemma 5.9. *$H^1(\ \langle\ \lambda^2 z, \frac{-1}{z} \mid (\frac{-1}{z} \circ \lambda^2 z)^2 = 1\ \rangle ; V\ )$ for $\lambda^2 \neq 1$ is trivial.*

Proof: Let $h(z) = \dfrac{-1}{z}$ and $g(z) = \lambda^2 z$. Then $hg = g^{-1}h$. We know that $F(h) = rz^2 + sz - r$ and $F(g) = kz^2 + w$.

$$\begin{aligned} F(hg) &= F(h)g + F(g) = [r(\lambda^2 z)^2 + s(\lambda^2 z) - r]\lambda^{-2} + (kz^2 + w) \\ &= r\lambda^2 z^2 + sz - r\lambda^{-2} + kz^2 + w = (r\lambda^2 + k)z^2 + sz + (w - r\lambda^{-2}). \end{aligned}$$

$$F(g^{-1}) = -F(g)g^{-1} = -\left[k\left(\frac{z}{\lambda^2}\right)^2 + w\right]\lambda^2 = -k\lambda^{-2}z^2 - w\lambda^2.$$

$$\begin{aligned} F(g^{-1}h) &= F(g^{-1})h + F(h) = \left[-k\lambda^{-2}\left(\frac{-1}{z}\right)^2 - w\lambda^2\right]z^2 + (rz^2 + sz - r) \\ &= (r - w\lambda^2)z^2 + sz + (-r - k\lambda^{-2}). \end{aligned}$$

In particular, we have $k = r - w\lambda^2 - r\lambda^2$. Since $F(h) = rz^2 + sz - r$ and $F(g) = [r - \lambda^2(r+w)]z^2 + w$, $\dim(Z^1(G;V)) \leq 3$. The result follows since $B^1(G;V)$ has dimension 3. $\square$

Lemma 5.10. *If G is a Borel subgroup of $PSL_2(p^n)$ and $p \neq 3$, then $H^1(G;V)$ is one dimensional if $p = 5$ and trivial otherwise. The parabolic cohomology of G with V coefficients is trivial.*

Proof: Let $u = 1+p+p^2+\cdots+p^{n-1}$. We may assume $G = < z+1, \lambda^2 z >$ where $< \lambda >= (\mathbb{F}_q)^\times$. Note that $< \lambda^u > = (\mathbb{F}_p)^\times$.

Let $g(z) = \lambda^2 z$ and $h(z) = z+1$. Then $g^u h = h^{\lambda^{2u}} g^u$. Moreover, $F(g) = mz^2 + w$ and $F(z+1) = rz^2 + sz + t$.

Now $g^u(z) = \lambda^{2u}(z)$. As in the proof of (5– 6) we get

$$\begin{aligned} F(g^u) &= F(g) + F(g)g + F(g)g^2 + \cdots + F(g)g^{u-1} \\ &= m\left(\frac{1-\lambda^{2u}}{1-\lambda^2}\right) z^2 + w\left(\frac{1-\lambda^{-2u}}{1-\lambda^{-2}}\right). \end{aligned}$$

Also $h^k(z) = z+k$ and $F(h)(h^k) = rz^2 + (2rk+s)z + (rk^2+sk+t)$ by Remark 5.1. Let $\ell = \lambda^{2u}$.

Now

$$\begin{aligned} F(h^\ell) &= F(h) + F(h)h + F(h)h^2 + \ldots + F(h)h^{\ell-1} \\ &= (rz^2+sz+t) + (rz^2+(2r+s)z+(r+s+t)) \\ &\qquad + \ldots + (rz^2 + (2r(\ell-1)+s)z + (r(\ell-1)^2 + s(\ell-1)+t)) \\ &= \ell rz^2 + \left(\ell s + 2r\left(\frac{\ell(\ell-1)}{2}\right)\right) z \\ &\qquad + \left(\ell t + \frac{s\ell(\ell-1)}{2} + r(1+2^2+3^2+\cdots+(\ell-1)^2)\right) \\ &= \ell rz^2 + (\ell s + r\ell(\ell-1))z + \left(\ell t + \frac{s\ell(\ell-1)}{2} + \frac{r\ell(\ell-1)(2\ell-1)}{6}\right). \end{aligned}$$

$$
\begin{aligned}
F(g^u h) &= F(h) \;+\; F(g^u)h \\
&= (rz^2+sz+t) \;+\; \left(m\left(\frac{1-\lambda^{2u}}{1-\lambda^2}\right)z^2 \;+\; w\left(\frac{1-\lambda^{-2u}}{1-\lambda^{-2}}\right)\right)(h) \\
&= (rz^2+sz+t) \;+\; (m\left(\frac{1-\lambda^{2u}}{1-\lambda^2}\right)z^2 \;+\; 2m\left(\frac{1-\lambda^{2u}}{1-\lambda^2}\right)z \\
&\qquad + \left(m\left(\frac{1-\lambda^{2u}}{1-\lambda^2}\right)\right) \;+\; w\left(\frac{1-\lambda^{-2u}}{1-\lambda^{-2}}\right)
\end{aligned}
$$

$$
\begin{aligned}
&= \left(r+m\left(\frac{1-\ell}{1-\lambda^2}\right)\right)z^2 \;+\; \left(s+2m\left(\frac{1-\ell}{1-\lambda^2}\right)\right)z \\
&\qquad + \left(t+m\left(\frac{1-\ell}{1-\lambda^2}\right)+w\left(\frac{1-\ell^{-1}}{1-\lambda^{-2}}\right)\right).
\end{aligned}
$$

$$
\begin{aligned}
F(h^\ell g^u) &= F(g^u) \;+\; F(h^\ell)g^u \\
&= \left(m\left(\frac{1-\lambda^{2u}}{1-\lambda^2}\right)z^2 \;+\; w\left(\frac{1-\lambda^{-2u}}{1-\lambda^{-2}}\right)\right) + \ell^2 rz^2 \;+\; (\ell s + r\ell(\ell-1))z \\
&\qquad + \left(\ell t + \frac{s\ell(\ell-1)}{2} + \frac{r\ell(\ell-1)(2\ell-1)}{6} \right)\ell^{-1} \\
&= \left(m\left(\frac{1-\ell}{1-\lambda^2}\right) + \ell^2 r \right)z^2 \;+\; (\;\ell s \;+\; r\ell(\ell-1)\;)z \\
&\qquad + \left(w\left(\frac{1-\ell^{-1}}{1-\lambda^{-2}}\right) + \frac{s(\ell-1)}{2} + t + \frac{r(\ell-1)(2\ell-1)}{6} \right).
\end{aligned}
$$

Equating the coefficients of z^2 in $F(h^\ell g^u)$ and $F(g^u h)$ gives $\ell^2 r = r$ which implies that $\ell^2 = 1$ or $r = 0$. Since $p \neq 3$ and λ^u has order $p-1$, $(\lambda^u)^4 = \ell^2 = 1$ if and only if $p = 5$. Therefore, $r = 0$ unless $p = 5$.

Assume $p \neq 5$. Equating the constant terms of $F(h^\ell g^u)$ and $F(g^u h)$ gives $\dfrac{s(\ell-1)}{2} = m\left(\dfrac{1-\ell}{1-\lambda^2}\right)$ which implies that $s = \dfrac{2m}{\lambda^2-1}$. Thus, $F(g) =$

$mz^2 + w$ and $F(z+1) = \left(\dfrac{2m}{\lambda^2 - 1}\right) z + t$. Consequently, $\dim(Z^1(G;V)) \leq 3$. But $\dim(B^1(G;V)) = 3$. Hence, $H^1(G;V) = \{0\} = PH^1(G;V)$ if $p \neq 3$ and $p \neq 5$.

Assume $p = 5$. Equating the coefficients of z in $F(h^\ell g^u)$ and $F(g^u h)$ gives

$$\begin{aligned} \ell s + r\ell(\ell - 1) &= s + 2m\left(\frac{1-\ell}{1-\lambda^2}\right) \\ \Longrightarrow \ \ell s - s &= \frac{2m(\ell - 1)}{\lambda^2 - 1} + r(\ell - 1) \\ \Longrightarrow \ s &= \frac{2m}{\lambda^2 - 1} + r. \end{aligned}$$

Equating the constant terms of $F(h^\ell g^u)$ and $F(g^u h)$ gives

$$\frac{m(\ell - 1)}{\lambda^2 - 1} = \frac{s(\ell - 1)}{2} + \frac{r(\ell - 1)(2\ell - 1)}{6}$$

or equivalently,

$$\begin{aligned} \frac{m}{\lambda^2 - 1} &= \frac{r(2\ell - 1)}{6} + \frac{m}{\lambda^2 - 1} + \frac{r}{2} \\ &= \frac{m}{\lambda^2 - 1} + \frac{r(1 + \ell)}{3}. \end{aligned}$$

Since $p = 5$, $\ell^2 = 1$ and therefore $\ell = -1$. Consequently, the above equation doesn't give any further restrictions on m or r. So $F(g) = mz^2 + w$ and $F(h) = rz^2 + \left(\dfrac{2m}{\lambda^2 - 1}\right) z + t$. Then $\dim(Z^1(G;V)) = 4$ and $\dim(PZ^1(G;V)) = 3$ by Remark 5.7. Hence, $\dim(H^1(G;V)) = 1$ and $PH^1(G;V)$ is trivial. $\square$

We will now compute the cohomology of any exceptional subgroup G of $PSL_2(\mathbb{F})$. As noted above, we may assume $G = \left\langle A = \dfrac{-1}{z}, B = \begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix} \right\rangle$

where $a^2 - a + 1 = 0$ and $b = 1$ if G is tetrahedral, $b^2 = 2$ if G is octahedral, $b^2 - b - 1 = 0$ if G is icosahedral.

We note the following simple but useful facts for future reference:

$$\boxed{a^2 = a - 1, \quad a^2 + 1 = a, \quad a^2 - a = -1, \quad a + a^{-1} = 1}$$

$$\boxed{a^3 = -1 = a^{-3}, \quad a^3 + 1 = 0 = a^{-3} + 1, \quad a^{-2} + 1 = a^{-1}}$$

$$\boxed{a^{-2} + a = 0, \quad a^{-3} + 2a^{-1} = a^{-2} + a^{-1}}$$

If $b^2 - b - 1 = 0$, then $b^2 = b + 1$ and

$$\boxed{b^3 = 2b + 1, \quad b^4 = 3b + 2, \quad b^5 = 5b + 3, \quad b^6 = 8b + 5}$$

$$\boxed{b^8 = 21b + 13, \quad b^2 + 1 = b + 2, \quad b^2 - 1 = b, \quad 1 - 2b^2 = -(2b + 1)}$$

$$\boxed{b^4 - b^2 + 2 = 2b + 3, \quad b^4 - b^2 - 1 = 2b}.$$

$F(A) = kz^2 + mz - k$. Let $F(B) = rz^2 + sz + t$. Using $(**)$, we have

$$\begin{aligned}
F(B^2) &= F(B) + F(B)B \\
&= (rz^2 + sz + t) + (\, ra^2z^2 + (2rab + s)z + (rb^2 + sba^{-1} + ta^{-2})\,) \\
&= r(a^2 + 1)z^2 + 2(rab + s)z + (rb^2 + sba^{-1} + t(a^{-2} + 1)) \\
&= raz^2 + 2(abr + s)z + (rb^2 + sa^{-1}b + a^{-1}t).
\end{aligned}$$

Now $B^2 = \begin{bmatrix} a^2 & b(a + a^{-1}) \\ 0 & a^{-2} \end{bmatrix} = \begin{bmatrix} a^2 & b \\ 0 & a^{-2} \end{bmatrix}$. Therefore, by $(**)$

$$\begin{aligned}
F(B^3) &= F(BB^2) = F(B^2) + F(B)B^2 \\
&= ra(a^3 + 1)z^2 + (2rba(a + 1) + 3s)z + (2rb^2 + sb(a^{-1} + a^{-2}) \\
&\qquad + ta^{-1}(1 + a^{-3})) \\
&= (2ra(a + 1)b + 3s)z + (2rb^2 + sb(a^{-1} + a^{-2})).
\end{aligned}$$

Since $B^3 = 1$, we have $F(B^3) = F(1) = 0$. Note that $a = -1$ if and only if $p = 3$.

If $p = 3$, then $B(z) = z - b$ is parabolic and therefore $r = 0$. In this case, $F(B^3) = 0$ gives no further restrictions. Thus,

$$\boxed{F(B) = sz + t \;\; \text{when } p = 3}\,.$$

If $p \neq 3$, then $2ra(a+1)b + 3s = 0 \implies s = \dfrac{-2ra(a+1)b}{3}$. Then

$$\begin{aligned} 2rb^2 + sb(a^{-2} + a^{-1}) &= 2rb^2 - \frac{2rb^2(a^{-1}+1)(a+1)}{3} \\ &= 2rb^2 - 2rb^2 = 0 \;\; (\text{since } a + a^{-1} = 1). \end{aligned}$$

So we get no further restrictions on $F(B)$ and

$$\boxed{F(B) \;=\; rz^2 - \left(\frac{2ra(a+1)b}{3}\right) z + t \;\; \text{when} \;\; p \neq 3}\,.$$

We therefore have $\dim(Z^1(G;V))$ is at most 4 and $\dim(B^1(G;V)) = 3$. Consequently, if there are any further relations between the coefficients of $F(A)$ and $F(B)$, then $H^1(G;V)$ is trivial.

Now

$$\begin{aligned} F(AB) &= F(A)B \;+\; F(B) \\ &= ka^2z^2 + (2kab + m)z + (kb^2 + ma^{-1}b - ka^{-2}) \;+\; F(B). \end{aligned}$$

Thus,

$$\boxed{F(AB) \;=\; (ka^2 + r)z^2 \;+\; (2kab + m + s)z \;+\; (kb^2 + ma^{-1}b - ka^{-2} + t)}$$

where $r = 0$ and $a = -1$ if $p = 3$ and $s = \dfrac{-2ra(a+1)b}{3}$ if $p \neq 3$.

Let $F(AB) = uz^2 + vz + w$. Let $F((AB)^n) = P_n z^2 + Q_n z + R_n$ for $n = 2,3,4,5$. Since $AB = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix} = \begin{bmatrix} 0 & -a^{-1} \\ a & b \end{bmatrix}$, (**) gives

$$
\begin{aligned}
F((AB)^n) &= F((AB)^{n-1})(AB) + F(AB) \\
&= (R_{n-1}a^2z^2 + (2R_{n-1}ab - Q_{n-1})z + (P_{n-1}a^{-2} - a^{-1}bQ_{n-1} + R_{n-1}b^2)) \\
&\qquad + (uz^2 + vz + w)
\end{aligned}
$$

which gives $F((AB)^n) =$

$$
\boxed{(R_{n-1}a^2 + u)z^2 + (2R_{n-1}ab - Q_{n-1} + v)z + (P_{n-1}a^{-2} - Q_{n-1}a^{-1}b + R_{n-1}b^2 + w)}.
$$

Remark 5.11 We obtain the following values of P_i, Q_i, R_i by reiteration:

i) $P_2 = u + a^2w$

ii) $Q_2 = 2abw$

iii) $R_2 = w + a^{-2}u - a^{-1}bv + b^2w$

iv) $P_3 = 2u - abv + a^2(b^2+1)w$

v) $Q_3 = 2a^{-1}bu + v(1-2b^2) + 2ab^3w$

vi) $R_3 = a^{-2}(b^2+1)u - a^{-1}b^3v + (b^4 - b^2 + 2)w$

vii) $P_4 = (b^2+2)u - ab^3v + a^2(b^4 - b^2 + 2)w$

viii) $Q_4 = 2a^{-1}b^3u + 2b^2(1-b^2)v + 2ab(b^4 - 2b^2 + 2)w$

ix) $R_4 = a^{-2}(b^4 - b^2 + 2)u - a^{-1}b(b^4 - 2b^2 + 2)v + (b^6 - 3b^4 + 3b^2 + 2)w$

x) $P_5 = (b^4 - b^2 + 3)u - ab(b^4 - 2b^2 + 2)v + a^2(b^6 - 3b^4 + 3b^2 + 2)w$

If $b^2 - b - 1 = 0$, then $P_5 = 2(b+2)u - a(3b+1)v + 2a^2(b+2)w$.

xi) $Q_5 = 2a^{-1}b(b^4 - 2b^2 + 2)u - (2b^6 - 6b^4 + 6b^2 - 1)v + 2ab^3(b^4 - 4b^2 + 5)w$

If $b^2 - b - 1 = 0$, then $Q_5 = 2a^{-1}(3b+1)u - (4b+3)v + 2a(3b+1)w$.

xii) $R_5 = a^{-2}(b^6 - 3b^4 + 3b^2 + 2)u - a^{-1}b^3(b^4 - 4b^2 + 5)v + (b^8 - 5b^6 + 8b^4 - 3b^2 + 3)w$

If $b^2 - b - 1 = 0$, then $R_5 = 2a^{-2}(b+2)u - a^{-1}(3b+1)v + 2(b+2)w$.

If G is tetrahedral, then $(AB)^3 = 1$ and $b = 1$. Since $0 = F((AB)^3) = P_3z^2 + Q_2z + R_2$,

$$\begin{aligned} 0 = P_3 &= 2u - av + 2a^2w \\ &= 2(ka^2 + r) - a(2ka + m + s) + 2a^2(k + ma^{-1} - ka^{-2} + t) \\ &= 2a^2k + am - as + 2r - 2k + 2a^2t. \end{aligned}$$

Therefore, $s = 2ak + m + 2a^{-1}r - 2a^{-1}k + 2at$. This gives a nontrivial relation for all p and thus $H^1(G;V) = \{0\}$ in all cases.

If G is octahedral, then $(AB)^4 = 1$ and $b^2 = 2$. Therefore,

$$\begin{aligned} 0 = P_4 &= 4u - 2abv + 4a^2w \\ &= 2a^2k + abm - abs + 2r - 2k + 2a^2t. \end{aligned}$$

Therefore, $s = 2ab^{-1}k + m + 2ra^{-1}b^{-1} - 2a^{-1}b^{-1}k + 2ab^{-1}t$. This gives a nontrivial relation for all p and thus $H^1(G;V) = \{0\}$ in all cases.

If G is icosahedral, then $0 = P_5 = Q_5 = R_5$ and $b^2 - b - 1 = 0$. Note that $b = -2$ if and only if $p = 5$.

If $p = 5$, we see from Remark 5.11 that $P_5 = Q_5 = R_5$ independently of what u, v, and w are. I.e., these give no further restrictions on $F(A)$ and $F(B)$.

Consequently, $\dim(Z^1(G;V)) = 4$ and $H^1(G;V)$ is one-dimensional. Since $p = 5$ and $|AB| = 5$, AB is a parabolic element. Thus, if $F \in PZ^1(G;V)$, then the coefficient of z^2 in $F(AB)$ must be zero. Therefore, $ka^2 + r = 0 \implies r = -ka^2$. Hence, $\dim(PZ^1(G;V)) = 3$ and $PH^1(G;V) = \{0\}$.

If $p \neq 5$, then

$$0 = P_5 = 2(b+2)(ka^2+r) - a(3b+1)(2kab+m+s) + 2a^2(b+2)(kb^2+ma^{-1}b-ka^{-2}+t).$$

Since $2a^2(b+2) \neq 0$, we can write t in terms of k, r, m, s, a and b. Hence, $H^1(G;V)$ is trivial if $p \neq 5$.

We have proved the following theorem.

Theorem 5.12. *The Eichler cohomology of every exceptional subgroup of $PSL_2(q)$ with $V_2(\mathbb{F}_q)$ coefficients except the icosahedral subgroups when $p = 5$ is trivial. The cohomology of the latter is one- dimensional.*

Theorem 5.13. *The Eichler cohomology of $PSL_2(p)$ with coefficients in $V_2(\mathbb{F}_q)$ is one-dimensional if $p = 5$ and trivial otherwise. The parabolic cohomology of $PSL_2(p)$ with $V_2(\mathbb{F}_q)$ coefficients is trivial for all p.*

Proof: We may assume $G := PSL_2(p) = \left\langle z+1, \dfrac{-1}{z} \right\rangle$. Let $g(z) = \dfrac{-1}{z}$ and $h(z) = z + 1$. Then $(gh)^2 = h^{-1}g$. Moreover, $F(g) = rz^2 + sz - r$ and $F(z+1) = kz^2 + mz + n$.

Note that $h^{-1}(z) = z - 1$ and $gh(z) = \dfrac{-1}{z+1}$. Therefore,

$$\begin{aligned}
F(h^{-1}) &= -F(h)h^{-1} = -kz^2 + (2k-m)z + (m-k-n), \\
F(gh) &= F(g)h + F(h) = (r+k)z^2 + (2r+s+m)z + (s+n), \\
F((gh)^2) &= F(gh)(gh) + F(gh) \\
&= (r+k+s+n)z^2 + 2(s+n)z + (-r+k-m+s+2n).
\end{aligned}$$

On the other hand,

$$F(h^{-1}g) = F(h^{-1})g + F(g) = (r+m-k-n)z^2 + (s-2k+m)z + (-r-k).$$

In particular, $r+k+s+n = r+m-k-n$ which implies that $s = m-2k-2n$. The equations $2(s+n) = s-2k+m$ and $-r+k-m+s+2n = -r-k$ are then trivially satisfied. Therefore, we have $F(g) = rz^2 + (m-2k-2n)z - r$ and $F(h) = kz^2 + mz + n$. Hence, the dimension of $Z^1(G;V)$ is at most 4. We also know that $B^1(G;V)$ is three- dimensional.

If $p = 3$, then $k = 0$ since h is parabolic. Therefore, the cohomology of G is trivial.

Assume $p \neq 3$. Note that $PH^1(G;V) = \{0\}$ (k must be 0). Suppose $\dim(H^1(G;V)) = 1$. Since the parabolic cohomology of G is trivial, there must exist a $[T] \in H^1(G;V)$ such that T is not a coboundary when restricted to parabolic elements. Consequently, $0 \neq [T|_B] \in H^1(B;V)$ where B is a Borel subgroup of G containing T. This is a contradiction to Lemma 5.10 unless $p = 5$. Hence, $H^1(G;V)$ is trivial unless $p = 5$.

When $p = 5$, $PSL_2(p) = PSL_2(5) \cong Alt(5)$. Therefore, $\dim(H^1(G;V)) = 1$ by Theorem 5.12. $\square$

Summary:

The dimension of $H^1(G;V)$ is one for the following subgroups of $PSL_2(q)$

i) $\langle\ z+1\ \rangle$ when $p \neq 3$

ii) $\left\langle\ z+1, \lambda^2 z\ \right\rangle$ when $p=5$

iii) icosahedral subgroups when $p=5$

iv) $PSL_2(p)$ when $p=5$

The dimension of $H^1(\{\ z+b \mid b \in \mathbb{F}_q\ \};V)$ is $3n-2$.

The dimension of $PH^1(\{\ z+b \mid b \in \mathbb{F}_q\ \};V)$ is $2n-2$

The cohomology and parabolic cohomology with $V_2(\mathbb{F}_q)$ coefficients of every other subgroup listed in Remark 5.2 is trivial.

Addendum

We recently became aware of the work of Audrey Terras and her students. In [T], Terras defines the **finite Poincaré upper half-plane** as

$$H_q = \{ z = x + y\sqrt{\delta} \mid x, y \in \mathbb{F}_q \text{ and } y \neq 0 \}$$

where q is an odd prime and $<\delta> = (\mathbb{F}_q)^\times$. Moreover, she defines the **Poincaré distance** between $z, w \in H_q$ to be

$$d(z,w) = \frac{N(z-w)}{(\mathrm{Im} z)(\mathrm{Im} w)}$$

where $z = x+y\sqrt{\delta}$, $\mathrm{Re} z := x$, $\mathrm{Im} z := y$, $\overline{z} := x - y\sqrt{\delta}$ and Nz = **Norm of** $z := z\overline{z}$.

Our definition of hyperbolic distance agrees with this one up to a scalar. However, we define distance using only conjugation which does not require a choice of coordinates (δ).

For a fixed $a \in \mathbb{F}_q$, Terras defines the **finite upper-half plane graph** $P_q(\delta, a)$ with vertex set H_q and with edge set $\{ (z,w) \mid d(z,w) = a \}$. If $a \notin \{0, 4\delta\}$, she proves that $P_q(\delta, a)$ is a connected graph of degree $q+1$. This is accomplished by realizing $P_q(\delta, a)$ as the Cayley graph of the Borel group $\{ \left(\begin{smallmatrix} y & x \\ 0 & 1 \end{smallmatrix}\right) \mid x, y \in \mathbb{F}_q, y \neq 0\}$ with respect to the set $R_q(\delta, a) = \{ z \in H_q \mid d(z, \sqrt{\delta}) = a \}$ (which is closed under inversion and is a generating set when $a \notin \{0, 4\delta\}$).

Here again, these graphs require only one parameter (a) using our definition of hyperbolic distance. Let Γ_a denote the graph with vertex set $\mathbb{H}$ and edge set $\{ (z,w) \mid \triangle'(z,w) = a \}$. Terras' case $a = 4\delta$ corresponds to $a = -1$ in our set-up.

Let $X = (V, E)$ be a finite k-regular connected graph.

The **adjacency matrix** A of X is indexed by V and has entries

$$a_{ij} = \begin{cases} 1 & \text{if } \{i,j\} \in E \\ 0 & \text{otherwise} \end{cases}$$

Reordering the vertices corresponds to conjugating A by a permutation matrix.

Note that A is symmetric with all diagonal entries equal to 0. Moreover, $A^n(v,w)$ (the entry of A^n indexed by v and w) is the number of paths of length n from v to w.

Fix an orientation on the edges of X and let $\widetilde{X}$ be the set of oriented edges. Let $e = (e_0, e_1) \in \widetilde{E}$.

Let D be the matrix with rows indexed by V, columns indexed by $\widetilde{E}$, and entries

$$a_{ve} = \begin{cases} -1 & v = e_0 \\ 0 & v \notin e \\ 1 & v = e_1 \end{cases}$$

Note that $DD^t = kI - A$.

Even though D depends on the choice of orientation, DD^t does not. DD^t is called the **combinatorial Laplacian** of X.

D is the matrix of the operator $d : \mathbb{C}^V \longrightarrow \mathbb{C}^E$ defined by $(df)(e) = f(e_1) - f(e_0)$. (Here $\mathbb{C}$ can be replaced by $\mathbb{R}$.)

Since DD^t is symmetric it has real eigenvalues and the eigenspaces are orthogonal with respect to the standard (hermitian) inner product on $\mathbb{C}^V$:

$$< f, g > = \sum_{v \in V} f(v)\overline{g(v)}.$$

In fact, the eigenvalues are nonnegative.

The eigenspace of the eigenvalue 0 is exactly the constant functions on V.

If λ is any other eigenvalue of DD^t and f is an eigenvector for λ, then $(kI - A)f = \lambda f$. Assume $f(v) \geq |f(w)|$ for all $w \in V$. Then

$$\begin{aligned} \lambda f(v) \; &= \; kf(v) - (Af)(v) \leq |kf(v) - (Af)v| \\ &\leq kf(v) + |(Af)(v)| \\ &\leq kf(v) + kf(v) \; = \; 2kf(v). \end{aligned}$$

Thus, $0 < \lambda \leq 2k$. In fact, $2k$ is an eigenvalue if and only if X is bipartite.

X is a **Ramanujan** graph if every eigenvalue of DD^t other than 0 and $2k$ satisfies $|\lambda - k| \leq 2\sqrt{k-1}$ [L2].

X is a c-**expander** (for $c \in (0, \infty)$) if for every subset Y of X, $|\partial Y| \geq c\left(1 - \frac{|Y|}{|X|}\right)|Y|$ where $\partial Y \; = \; \{\, z \in X \mid d(z, Y) = 1 \,\}$ is the **boundary** of Y.

A family of expanders is a family of k-regular graphs (for fixed k and with the number of vertices going to infinity) which are all c-expanders for the same c.

A family of (n, k, c)-expanders where the number of vertices n goes to infinity, k and c are fixed and c is as large as possible play a very important role in computer science. They are used in building communication networks among other things. It is known that expanders exist [L2] but explicit construction of these graphs is necessary for applications. Ramanujan graphs are known to be the best possible expanders for graphs of fixed degree. The first explicit constructions of k-regular Ramanujan graphs were given by Lubotsky, Phillips and Sarnak [L2]. Following the work of Soto-Andrade and Katz, Terras' conjecture that Γ_a is Ramanujan for $a \in (\mathbb{F}_q)^\times - \{-1\}$ has been established.

Let $\mathbb{F} = \mathbb{F}_q$ for the remainder of this section.

It is still an open question whether the $q-2$ graphs Γ_a, $a \in \mathbb{F}^\times - \{-1\}$ are isomorphic or not [T]. Terras mentions that there are three nonisomorphic graphs when $q = 5$. We will now show that there are always at least three nonisomorphic graphs when $q > 3$.

Lemma A.1. *Given $a \in \mathbb{F}^\times$, there are three possibilities:*

i) *There is no hyperbolic equilateral triangle with side lengths a.*

ii) *Every hyperbolic equilateral triangle with side lengths a is degenerate.*

iii) *Every hyperbolic equilateral triangle with side lengths a is nondegenerate.*

Moreover, all three possibilities occur if $q > 3$.

Proof: Let $a \in \mathbb{F}^\times - \{-1\}$. Suppose there exists an equilateral hyperbolic triangle with side lengths a. Working in the disk model, we may assume the triangle is $(0, P, Q)$. Since $\mathbb{S}z$ acts transitively on the circle $\{ z \in \mathbb{D} \mid \triangle(0,z) = a \}$, $Q = sP$ where $s \in \mathbb{S} - \{1\}$.

Now $s = -1$ if and only if $(0, P, Q)$ is degenerate.

$$\triangle(0,P) = \frac{P\overline{P}}{1 - P\overline{P}}, \qquad \triangle(P, sP) = \frac{P\overline{P}(2 - s - \overline{s})}{(1 - P\overline{P})^2}.$$

Therefore, $\triangle(0,P) = a = \triangle(P, sP)$ if and only if $P\overline{P} = (s + \overline{s}) - 1$.

Thus, $(0, P, Q)$ is degenerate if and only if $s = -1$ if and only if $a = \frac{-3}{4}$.

Consider the map $\phi : \mathbb{S} - \{\pm 1\} \longrightarrow \mathbb{F}$ given by $s \mapsto s + \bar{s}$.

If $s + \bar{s} = t + \bar{t}$, then $s - t = \bar{t} - \bar{s} = \dfrac{s-t}{st}$. This implies that $s = t$ or $s = \bar{t}$. Consequently, $\phi^{-1}(s + \bar{s}) = \{s, \bar{s}\}$. There are therefore $\dfrac{q-1}{2}$ pairs $\{s, \bar{s}\}$, each of which corresponds to a unique element $s + \bar{s}$ of $\mathbb{F}$. If $s + \bar{s} - 1 \notin \{0, 1\}$, then there exists a $P \in \mathbb{D}$ so that $P\overline{P} = s + \bar{s} - 1$ and $(0, P, sP)$ is a nondegenerate hyperbolic equilateral triangle with side lengths $a = \dfrac{P\overline{P}}{1 - P\overline{P}}$.

Now $s + \bar{s} - 1 \neq 1$ since $s \neq 1$. Moreover, $s + \bar{s} - 1 = 0$ if and only if $s + \bar{s} = 1$ if and only if $P\overline{P} = 0 = a$. So one of the pairs $\{s, \bar{s}\}$ will yield $a = 0$. Thus, there are $\dfrac{q-1}{2} - 1 = \dfrac{q-3}{2}$ a's in $\mathbb{F}^{\times} - \{-1\}$ for which there exists a nondegenerate hyperbolic triangle with side lengths a and one a $(= \frac{-3}{4})$ for which there exists a degenerate hyperbolic triangle with side lengths a. Since $q - 2 > \dfrac{q-1}{2}$ when $q > 3$, there must exist an $a \in \mathbb{F}^{\times} - \{-1\}$ for which there is no hyperbolic equilateral triangle with side lengths a. □

Theorem A.2. *There are at least three nonisomorphic graphs Γ_a, $a \in \mathbb{F}^{\times} - \{-1\}$ when $q > 3$.*

Proof: Let $a \in \mathbb{F}^{\times} - \{-1\}$. Let $A(a)$ denote the adjacency matrix of Γ_a.

Now the diagonal entries of $A^3(a)$ count the number of cycles of length 3 in Γ_a. Note that Γ_a has a cycle of length three if and only if there is an equilateral hyperbolic triangle with side lengths a.

By Lemma A.2, there exists an $a_1 \in \mathbb{F}^{\times} - \{-1\}$ for which no equilateral hyperbolic triangle with side lengths a_1 exists. Consequently, the trace of $A^3(a_1)$

is zero.

By Lemma A.2, there exists an $a_2 \in \mathbb{F}^\times - \{-1\}$ such that every hyperbolic equilateral triangle with side lengths a_2 is degenerate. Working in the disk model, we may assume 0 is a vertex. If we start at the vertex 0, there are $q+1$ choices for the next vertex P in the three cycle (since the degree of Γ_{a_2} is $q+1$). Since $(0, P, Q)$ must be degenerate where Q is the third vertex in the three cycle, $Q = -P$. Thus, there are exactly $q+1$ cycles of lengths three at 0. Consequently, the trace of $A^3(a_2)$ is $|V|(q+1)$ (by transitivity).

By Lemma A.2, there exists an $a_3 \in \mathbb{F}^\times - \{-1\}$ such that every hyperbolic equilateral triangle with side lengths a_2 is nondegenerate. Starting at the vertex 0, there are $q+1$ choices for the next vertex P in the three cycle. The third vertex Q in the three cycle must satisfy $\triangle(P, Q) = a$ and $\triangle(0, Q) = a$. In particular, $Q \in \{ z \mid \triangle(z, 0) = a \} \cap \{ z \mid \triangle(z, P) = a \}$. These two circles are distinct since one is a Euclidean circle centered at 0 and the other is not. Since $(0, P, Q)$ is nondegenerate, the two circles intersect in exactly two points. Thus, there are exactly $2(q+1)$ cycles of length three at 0 and the trace of $A^3(a_3)$ is $|V|2(q+1)$.

Since the trace of the adjacency matrix is an invariant of isomorphic graphs, Γ_1, Γ_2 and Γ_3 are all nonisomorphic. □

Let $T(2, m, n)$ denote the triangle group

$$< \rho,\ \sigma,\ \tau \mid \rho^2,\ \sigma^2,\ \tau^2,\ (\rho\sigma)^m,\ (\rho\tau)^n,\ (\sigma\tau)^2 >$$

and let

$$T^{+}(2,m,n) \;=<\; \alpha,\; \beta,\; \gamma \mid \alpha^2,\; \beta^m,\; \gamma^n,\; \alpha\beta\gamma\; >$$

be the orientation preserving subgroup of $T(2,m,n)$. (Here $\alpha = \sigma\tau,\ \beta = \tau\rho, \gamma = \rho\sigma$.)

Let $\phi : T^{+}(2,m,n) \longrightarrow G$ be a surjective homomorphism such that $|\phi(\alpha)| = 2$, $|\phi(\beta)| = m$, and $|\phi(\gamma)| = n$. Then $\operatorname{Ker}(\phi)\backslash\widetilde{X}$ is an orientable surface (with a hyperbolic structure if its genus is at least two) with a $T^{+}/\operatorname{Ker}(\phi)+ \cong G$ action where

$$\widetilde{X} \;=\; \begin{cases} S^2 & \text{if} \quad \dfrac{1}{m}+\dfrac{1}{n} > \dfrac{1}{2} \\ \mathbb{R}^2 & \text{if} \quad \dfrac{1}{m}+\dfrac{1}{n} = \dfrac{1}{2} \\ \mathbb{H}^2_{\mathbb{R}} & \text{if} \quad \dfrac{1}{m}+\dfrac{1}{n} < \dfrac{1}{2} \end{cases}$$

I.e., $\widetilde{X}$ is the universal cover of a surface of genus $0,1$ or ≥ 2, respectively.

Let D be a triangle in $\widetilde{X}$ with interior angles $\frac{\pi}{2}, \frac{\pi}{m}, \frac{\pi}{n}$. Then D is a fundamental domain for T. (The reflections through the sides of T are ρ, σ, τ.) Thus, we have a tiling of $\widetilde{X}$ by triangles with angles $\frac{\pi}{2}, \frac{\pi}{m}, \frac{\pi}{n}$.

Let A, B, C be the vertices of D at angles $\frac{\pi}{n}, \frac{\pi}{m}, \frac{\pi}{2}$ respectively. There are $2n$ tiles containing A since the angle at A is $\frac{\pi}{n}$. Note that D and $\tau(D)$ fit together at C to form an angle of π. (This is a fundamental domain for T^{+}.) Consequently, the union of the $2n$ tiles is an n-gon. (The four tiles containing C form a rhombus, not a square, as D and $\tau(D)$ do not form an angle of π at B.) Similarly, there are $2m$ tiles containing B whose union is an m- gon. Thus, we have two more tilings of $\widetilde{X}$, one by n-gons and one by m-gons.

Let $\widetilde{\Gamma}$ be the graph whose vertices are the n-gons (or their centroids) and with an edge between two n-gons if and only if they share a common side. $\widetilde{\Gamma}$ is an n-regular graph. Similarly, we can construct $\widetilde{\Gamma}^*$ using the m-gons. Note that the centroids of the n-gons are the vertices of the m-gons and there is an edge between two such centroids if and only if the n-gons are adjacent.

For example, when $m = 3$ and $n = 6$, we get a tesselation of the Euclidean plane by hexagons and one by equilateral triangles. The centers of the hexagons are the vertices of the triangles and vice-versa. The plane is tesselated by squares when $m = n = 4$. The sphere with the dual tesselations coming from the cases $(2,3,3), (2,3,4)$ and $(2,3,5)$ respectively is a tetrahedron (which is self-dual), a cube and its dual (the octahedron) or a dodecahedron and its dual (the icosahedron). All other cases give us a tesselation of the (classical) hyperbolic plane.

The projection of these graphs gives us dual graphs $\Gamma = \Gamma_{\phi} := \mathrm{Ker}(\phi)\backslash\widetilde{\Gamma}$ and $\Gamma^* := \mathrm{Ker}(\phi)\backslash\widetilde{\Gamma}^*$ on the surface $\mathrm{Ker}(\phi)\backslash\widetilde{X}$; i.e., the regions of one graph on the surface are the vertices of the dual and there is an edge between them.

The above gives a geometric construction of the Terras graph: Given any $2 < d$ dividing $p - 1$ where p is a prime and $q = p^n > 5$, there is a surjective homomorphism $\phi : T^+(2, d, q+1) \longrightarrow PGL_2(q)$ [OST]. The graph Γ constructed above for this case is the Terras graph. Given any edge $\{P, Q\}$ of a Terras graph, let $\phi(\alpha) = g$ where g is the unique element (necessarily of order 2) in $PGL_2(q)$ interchanging P and Q. Let $\phi(\gamma)$ be any generator of $PGL_2(\mathbb{F})_P \cong \mathbb{S}$, and

$d = |gh|$. Thus, we can recover the epimorphism $\phi : T^+(2, d, q+1) \longrightarrow PGL_2(q)$. Since the action of $PGL_2(q)$ is transitive on oriented edges, choosing a different edge has the effect of conjugating ϕ by an element of $PGL_2(q)$. Conversely, given $\Gamma = \Gamma_\phi$, we will determine the value of a such that Γ is Γ_a.

It is still unknown whether there are infinitely many k-regular Ramanujan graphs for all k [L]. Given a fixed d, there are infinitely many primes p such that $d|(p-1)$. Our construction gives an infinite family of graphs Γ^* for triangle groups $T^+(2, d, p+1)$. We conjecture that these graphs are also Ramanujan. If this can be proved, the above problem will be settled.

BIBLIOGRAPHY

[B] Beardon, Alan F., *The Geometry of Discrete Groups*, vol. 91, Springer-Verlag, New York Inc, 1993.

[Br] Brown, Kenneth S., *Cohomology of Groups*, Springer-Verlag, New York, 1982.

[D] Dickson, L.E., *Linear Groups with an Exposition of the Galois Field Theory*, Leipzig, B.G. Teubner, 1901.

[H] Hahn, Liang-shin, *Complex Numbers & Geometry*, Mathematical Association of America, Washington, DC, 1994.

[J] Jacobs, Harold R., *Geometry*, W.H. Freeman and Company, San Francisco, 1974.

[K] Katz, N., *Estimates for Soto-Andrade Sums*, J. reine angew. Math.438 (1993), 143-161.

[Kr] Kra, Irwin, *Automorphic Forms and Kleinian Groups*, W.A. Benjamin, Inc, Reading, Mass., 1972.

[L] Lubotzky, Alexander, *Cayley Graphs: Eigenvalues, Expanders and Random Walks, Survey in Combinatorics, LMS Lecture Notes 218* (Peter Rowlinson, ed.), Cambridge University Press, 1995, pp. 155-189.

[L2] Lubotzky, Alexander, *Discrete Groups, Expanding Graphs and Invariant Measures*, vol. 125, Progress in Mathematics, Birkhäuser Verlag, 1994.

[LPS] Lubotzky, A., Phillips, R. & Sarnak, P., *Ramanujan Graphs*, Combinatorica, 8 (1988), 261- 277.

[M] MacLane, Saunders, *Homology*, Springer, Berlin, 1963.

[OS] Ozaydin, M. & Simmons, C., *The Geometry of* $PSL_2(\mathbb{F})$, Preprint.

[OST] Ozaydin, M., Simmons, C. & Taback, J., *The Spherical Hurwitz Problem for* $PSL_2(q)$, Preprint.

[S-A] Soto-Andrade, J., *Geometrical Gel'fand Models, Tensor Quotients, and Weil Representations*, Proc. Symp. Pure Math 47, part 2 (1987), Amer. Math. Soc., Providence.

[S] Suzuki, Michio, *Group Theory*, vol. 2, Berlin; New York: Springer-Verlag, 1982.

[T] Terras, Audrey, *Survey of Spectra of Laplacians on Finite Symmetric Spaces*, Experimental Mathematics, 1 **5** (1996).

IMAGE EVALUATION TEST TARGET (QA-3)

150mm

6"