



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
POSGRADO CONJUNTO EN CIENCIAS MATEMÁTICAS
CENTRO DE CIENCIAS MATEMÁTICAS

TRES PLANOS PROYECTIVOS DE ORDEN 9

TESIS

QUE PARA OPTAR EL TÍTULO DE:
MAESTRA EN CIENCIAS MATEMÁTICAS

PRESENTA:
ESTEFANÍA GONZÁLEZ ARROYO

TUTOR:
DR. DANIEL PELLICER COVARRUBIAS
CENTRO DE CIENCIAS MATEMÁTICAS UNAM

Morelia, Michoacán, noviembre 2018



Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

Índice general

Agradecimientos	I
Resumen	III
Abstract	V
Introducción	VII
1. Planos proyectivos	1
1.1. Colineaciones	6
1.2. Planos desarguesianos	13
2. Planos proyectivos sobre campos	15
2.1. Proyectividades de $\Pi(K)$	17
2.2. Otra construcción de $\Pi(K)$	21
3. Casi-campos de 9 elementos.	23
3.1. El campo de orden 9	26
3.2. minicuaternios \mathcal{Q}	28
3.3. Automorfismos del casi campo de los minicuaternios.	30
3.4. Soluciones de ecuaciones en \mathcal{Q}	33
4. El plano Ω y Ω^D	37
4.1. Construcción de Ω	37
4.2. Plano dual Ω^D	41
4.3. Colineaciones en Ω	42

4.3.1. Colineación $\tau_{\varepsilon,\delta}$	42
4.3.2. Colineación $\zeta_{\rho,\sigma}$	44
4.3.3. Colineaciones \mathcal{R} y \mathcal{U}	45
4.3.4. Colineaciones dadas por automorfismos	46
4.4. Transitividad en Ω	47
Bibliografía	57

Agradecimientos

Agradezco al Programa UNAM-PAPIIT IN-100518, el cual me otorgo una beca para la realización de mi tesis de maestría.

A mi familia, mi mamá que siempre me ha dado todo, mis hermanos que me ayudan en todo y por suerte matemáticamente también.

A mi asesor el Doctor Daniel Pellicer, por su gran apoyo, por su tiempo, dedicación, orientación y paciencia durante la realización de mi tesis.

A mis sinodales los doctores Miguel, Edgardo, Gabriela y Ernesto, por sus oportunas correcciones.

A Manuel que ya padecido el estrés de dos tesis. Además de su apoyo incondicional. También gracias por ayudarme con la talacha.

Resumen

La presente tesis trata de la construcción de planos proyectivos. Damos una construcción general para los planos proyectivos sobre campos. Todos estos planos proyectivos son desarguesianos (cumplen con el teorema de Desargues).

El orden 9 es el primero para el cual hay planos proyectivos no desarguesianos, como todos los planos que se construyen sobre campos son desarguesianos, necesitamos otra estructura. Construiremos dos Ω y su dual planos Ω y su dual que no son desarguesianos. Estos se construyen sobre un casi-campo con 9 elementos que se llama minicuternios. Además existe otro plano no isomorfo a los anteriores, también construido sobre los minicuternios que es no desarguesiano.

plano, proyectivo, casi-campo, minicuternios, desarguesiano

Abstract

In this thesis we construct projective planes. We have a general construction of the planes over a field. Every projective plane over a field has the property of being desarguesian (this means that the Desargues' theorem holds).

In order 9 we have the first planes which aren't desarguesian, as all the planes over a field are desarguesian, to construct a no desarguesian plane we need other structure. The structure we use is a near-field called Miniquaternions. The projective plane Ω and its dual are no desarguesian planes. Also there is another plane not isomorphic to Ω and its dual.

Introducción

Dentro de las matemáticas discretas se han estudiado varias estructuras de incidencia consistentes de un conjunto de puntos y un conjunto de subconjuntos de puntos. Un ejemplo de ellas son las gráficas [2], que constan de un conjunto de puntos que son los vértices y un conjunto de aristas que son subconjuntos de dos vértices. Otros ejemplos son los matroides [3] y los diseños de bloques. Las estructuras de incidencia que son importantes para esta tesis son los planos proyectivos, y en menor medida los planos euclidianos, que están conformados por puntos y rectas (subconjuntos de puntos).

En el plano euclidiano real tenemos que por cualesquiera dos puntos diferentes pasa una única recta. Además dos rectas diferentes se intersectan en un único punto a menos que sean paralelas. Entonces, si agregamos una recta que contenga puntos de intersección para las rectas paralelas, obtendremos una estructura en la que cualesquiera dos rectas se intersectan en un único punto, que es conocida como el plano proyectivo real.

Podemos pensar a un plano proyectivo como un plano euclidiano agregándole una recta a la que llamamos recta al infinito conformada por los puntos de intersección de las rectas paralelas.

Es posible construir un plano euclidiano combinatorio a partir de cualquier campo, de manera análoga a la construcción sobre los reales. La definición combinatoria de plano euclidiano se basa en las incidencias de puntos y rectas de los planos euclidianos construidos sobre campos, pero hay estructuras que satisfacen estos axiomas, y por lo tanto son planos euclidianos combinatorios, sin embargo no pueden ser construidas a partir de campos.

En el capítulo 1 se probará que en los planos proyectivos finitos todas las rectas

tienen la misma cantidad de puntos, por lo que podemos definir el orden de un plano a partir de la cantidad de puntos que contiene una recta (uno menos que la cantidad de puntos).

En 1782 Euler propuso el problema de los treinta y seis oficiales, el cual pregunta si se pueden colocar 36 oficiales diferentes de 6 regimientos diferentes con 6 rangos diferentes en una cuadrícula de 6×6 de tal forma que en ninguna columna o renglón haya dos oficiales del mismo rango o regimiento. En 1901 Gaston Tarry probó que no se podía hacer el arreglo del problema de los 36 oficiales [9].

Determinar todos los planos proyectivos finitos sigue siendo un problema abierto. Por ejemplo se sabe que no hay un plano proyectivo de orden 6, porque esto implicaría que se puede resolver el problema de los 36 oficiales.

Los planos proyectivos que se obtienen a partir de un campo son "desarguesianos"[8], lo que quiere decir que en el plano tenemos la configuración del teorema de Desargues. Dicha propiedad afirma que cualesquiera dos triángulos en perspectiva desde un punto se encuentran en perspectiva desde una recta. En el capítulo 2 se abunda sobre la propiedad de ser desarguesiano.

Todos los planos proyectivos de orden a los más 8 son desarguesianos. Existen 4 planos proyectivos distintos de orden 9 (todos tienen 91 puntos). Uno es el plano proyectivo construido sobre el campo con 9 elementos y por lo tanto es desarguesiano. Los 3 restantes no son desarguesianos, y por lo tanto no pueden ser construidos a partir de un campo. Sin embargo los podemos construir sobre el casi-campo de los minicuaternios (que tiene 9 elementos). Un casi-campo es una estructura que como su nombre lo indica es casi un campo salvo algunos axiomas de conmutatividad y distributividad. Los minicuaternios reciben este nombre ya que su grupo multiplicativo es el grupo de los cuaternios.

Hanfried Lenz dio una clasificación de planos proyectivos en 1954 [6], que después fue mejorada por Adriano Barlotti en 1957 [7]. Los clasificaron mediante el grupo de colineaciones del plano proyectivo y los puntos y rectas para los cuales era transitivo. Esta clasificación es conocida como la clasificación de Lenz-Bartolli de planos proyectivos.

Los planos proyectivos que se presentan en este trabajo son principalmente los

de orden 9, que es el menor orden para el que existe un plano proyectivo no desarguesiano. Como dijimos hay 4 planos de orden 9: el que se construye sobre el campo con 9 elementos y que es autodual; un plano al que llamaremos Ω construido sobre los minicuaternios que es diferente a su dual Ω^D ; y un plano Ψ también construido sobre los Mincuaternios que es autodual.

El plano Ω se construye a partir de un plano afín construido sobre los minicuaternios y que luego se extiende a un plano proyectivo. A partir de éste construimos su plano dual Ω^D que no es isomorfo a Ω , lo cual se puede ver a partir de la (P, l) -transitividad de Ω y Ω^D para ciertos puntos y rectas. Estos dos planos son no desarguesianos.

Además de construirse completando el plano proyectivo real con una recta, el plano proyectivo real también se puede construir mediante coordenadas homogéneas en \mathbb{R}^3 . El plano Ψ se construye de forma parecida mediante coordenadas homogéneas de ternas ordenadas que tienen por entradas elementos de los minicuaternios. Este plano tampoco es desarguesiano. El plano Ψ no está presente en el desarrollo de este trabajo ya que incrementaría demasiado su contenido.

La presente tesis se basa en el libro *miniquaternion Geometry* [1]. En el primer capítulo damos la definición de plano proyectivo y sus propiedades básicas, además de hablar de las colineaciones. En el segundo capítulo analizamos dos casi-campos de orden 9, el campo finito de orden 9 y los minicuaternios. En el capítulo 3 vemos una construcción de los planos proyectivos sobre campos. Por último, en el capítulo 4 analizamos los planos Ω y Ω^D que no son desarguesianos.

Capítulo 1

Planos proyectivos

En este capítulo daremos las nociones básicas de planos proyectivos. En un plano proyectivo tenemos puntos y rectas (subconjuntos de puntos) y estudiamos sus relaciones de incidencia.

Definición. 1.1. Un *plano proyectivo* es un conjunto de puntos y rectas relacionados mediante incidencia, que cumple los siguientes axiomas:

- 1) Dados dos puntos hay una única recta que los contiene.
- 2) Dadas dos rectas hay exactamente un punto que pertenece a ambas.
- 3) Hay un conjunto de 4 puntos con la propiedad de que cualesquiera 3 no pertenecen a la misma recta.

Si un punto está en una recta se dice que está contenido o que pertenece a la recta.

El último axioma se pide para evitar a los planos degenerados [5].

Denotaremos a la única recta que pasa por los puntos A y B por AB , y $l \cap m$ al único punto en la intersección de las rectas l y m .

El plano de la figura 1.1 es conocido como el plano de Fano. El plano de Fano es un plano proyectivo. Tiene 7 puntos que son A, B, C, D, E, F, G . Sus 7 rectas tienen 3 puntos cada una, y son $\{A, B, C\}$, $\{C, F, G\}$, $\{C, D, E\}$, $\{B, F, D\}$, $\{A, F, E\}$, $\{B, G, E\}$ y $\{A, G, D\}$. Es fácil convencerse de que el plano de Fano cumple los 3 axiomas de plano proyectivo.

Definición. 1.2. Un *cuadrángulo regular* es un conjunto de cuatro puntos en los que no hay 3 que sean colineales, es decir, que satisfagan el axioma 3) de la definición

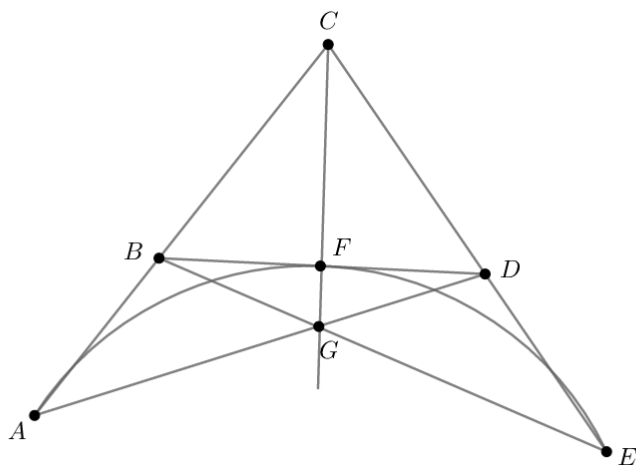


Figura 1.1: Plano de Fano

1.1.

Por ejemplo en el plano de Fano los puntos F, D, G y E forman un cuadrángulo regular (ver figura 1.1).

Gracias a la existencia de un cuadrángulo regular tenemos el siguiente lema.

Lema. 1.3. Dadas dos rectas diferentes en un plano proyectivo existe un punto que no pertenece a ninguna de ellas.

Demostración. Sean l y m dos rectas en un plano proyectivo. Por la existencia de un cuadrángulo regular (axioma 3) tenemos 4 puntos A, B, C y D que cumplen que no hay tres de ellos que sean colineales. Si alguno de estos puntos no está en l ni en m , es el punto buscado. En caso contrario tenemos A, B, C y D en $l \cup m$, pero no hay tres que pertenezcan a la misma recta. Digamos que A y C están en l y que B y D están en m (ver figura 1.2).

Las rectas AB y CD se intersectan en un punto P . Como A pertenece a l y B a m , entonces P no pertenece a l ni a m . ■

Definición. 1.4. Al conjunto de rectas que pasan por un punto lo llamamos *lápiz de rectas*.

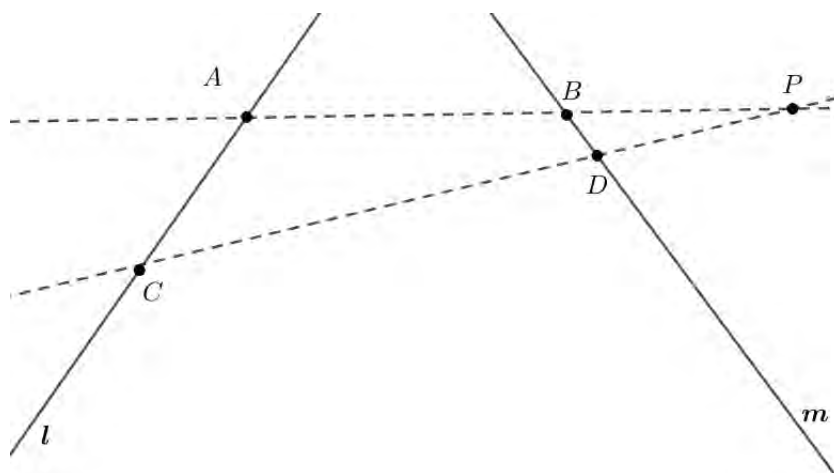


Figura 1.2:

A partir de un plano proyectivo Π podemos definir al *plano dual* Π^D , el cual tiene por puntos a las rectas de Π y las rectas son lápices de rectas por Π . Como las rectas en Π^D se corresponden con los puntos de Π se satisface que un punto es incidente a una recta en Π^D si y sólo si son incidentes en Π como recta y punto respectivamente.

Observación. 1.5. El plano de Fano es igual a su dual salvo por un reetiquetado de vértices (ver figura 1.3).

La dualidad puede usarse para construir nuevos planos proyectivos, como muestra el siguiente teorema.

Teorema. 1.6. Dado cualquier plano proyectivo Π su dual Π^D es un plano proyectivo.

Demostración. Probaremos los 3 incisos de las definición 1.1 se valen para Π^D .

Dos puntos L y M en Π^D son dos rectas en Π . Entonces hay un único punto P de Π en el que L y M se intersectan, por lo que este punto P es la única recta en Π^D que contiene a ambos puntos.

De manera análoga, por el axioma 1) de la definición de plano proyectivo tenemos que se cumple el axioma 2) en el plano dual; la recta que pasa por dos puntos P y Q en Π corresponde al punto de intersección de las rectas que representan a P y Q en Π^D .

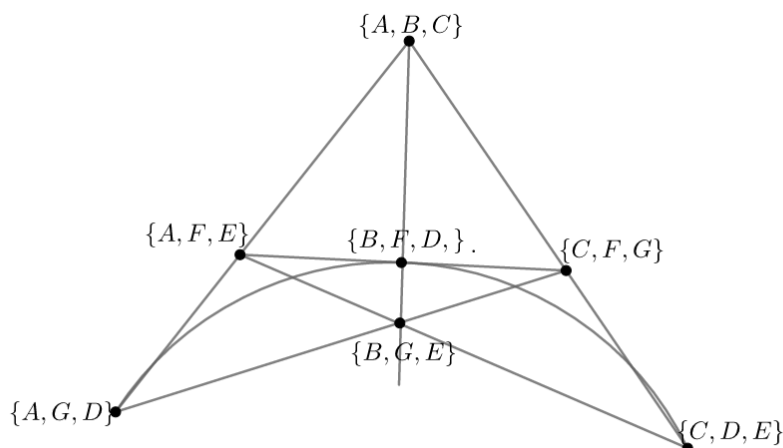


Figura 1.3: Dual del plano de Fano

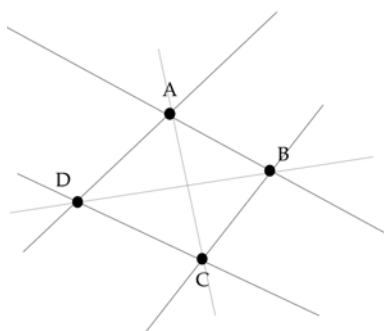


Figura 1.4: Cuadrángulo regular

Como Π es un plano proyectivo existe un cuadrángulo regular $ABCD$ (ver figura 1.4), entonces como en A, B, C, D no hay 3 puntos que sean colineales, en las rectas AB, BC, CD y DA no hay 3 que sean concurrentes; y por lo tanto en Π^D los puntos AB, BC, CD y DA son 4 puntos de Π^D de los cuales no hay 3 que sean colineales. ■

Los axiomas que debe satisfacer un plano proyectivo imponen varias restricciones sobre el número de puntos de cada recta, como muestran los siguientes resultados.

Proposición. 1.7. En un plano proyectivo finito se cumple que:

- i) Todas las rectas tienen el mismo número de puntos.
- ii) El número de puntos en una recta es igual al número de rectas que pasan por un

punto.

Demostración. Sean P y l un punto y una recta respectivamente, tales que $P \notin l$. Cada recta que pasa por P intersecta a la recta l en un único punto, entonces tenemos una correspondencia biyectiva entre los puntos de l y las rectas que pasan por P . Sea m una recta distinta de l y Q un punto que no pertenezca a ninguna de ellas, el cual existe por 1.3. Entonces las rectas que pasan por Q se corresponden biyectivamente con los puntos en l y con los puntos en m , por lo que l y m tienen el mismo número de puntos lo que prueba el primer inciso.

Como hemos visto, las rectas que pasan por un punto se corresponden biyectivamente con los puntos de una recta a la que no pertenezca el punto, pero como todas las rectas tienen la misma cantidad de puntos, se deduce ii). ■

Decimos que un plano proyectivo con una cantidad finita de puntos tiene *orden* k si cada recta tiene $k + 1$ puntos. Sabiendo el orden de un plano proyectivo podemos deducir el número de rectas y puntos que contiene.

Teorema. 1.8. Un plano proyectivo finito de orden k tiene $k^2 + k + 1$ rectas y $k^2 + k + 1$ puntos.

Demostración. Una recta l tiene $k + 1$ puntos y por cualquier punto pasan $k + 1$ rectas. Entonces tenemos $k + 1$ puntos en l por los que pasan k rectas distintas de l . Esto da en total $(k + 1)k$ rectas más la recta l , lo que nos da $k^2 + k + 1$ rectas distintas. De lo anterior es fácil ver que hay $k^2 + k + 1$ puntos, ya que tenemos $k^2 + k + 1$ rectas con $k + 1$ puntos, pero cada punto está en $k + 1$ rectas. ■

Definición. 1.9. Dos planos proyectivos son *isomorfos* si hay una biyección entre los conjuntos de puntos tal que los puntos de una recta tienen por imágenes los puntos de una recta.

No hay planos proyectivos de orden 1 ya que los planos proyectivos tienen al menos 4 puntos. Veamos que hay un único plano de orden 2 salvo isomorfismo. Si Π es un plano proyectivo de orden 2, entonces tiene 7 puntos digamos A, B, C, D, E, F, G . Cada recta tiene 3 puntos y por cada punto pasan 3 rectas diferentes. Como en la figura 1.1, tomemos como rectas por A a los conjuntos $\{A, B, D\}$, $\{A, G, C\}$, $\{A, E, F\}$.

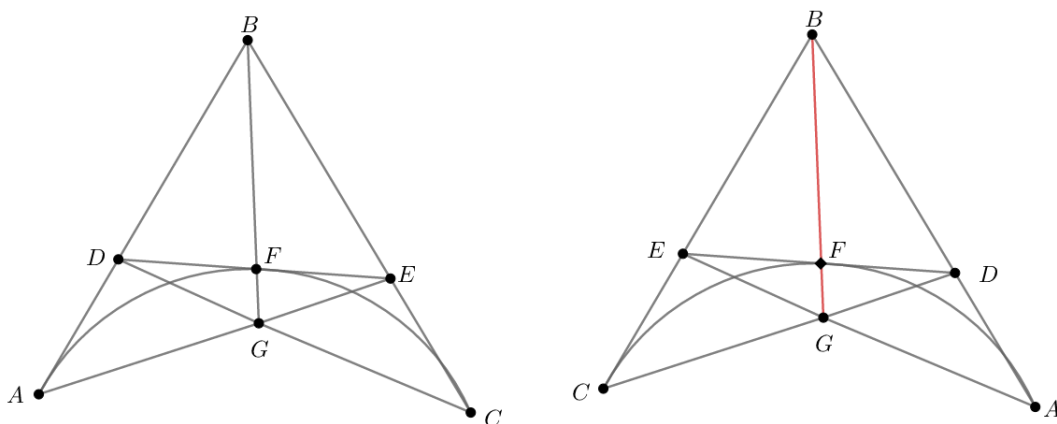


Figura 1.5: Colineación en el plano de Fano

La recta que une a B y C tiene que intersectar a $\{A, E, F\}$ en un punto diferente de A ; tomemos E como el punto de intersección de las rectas BC y AE . De lo anterior tenemos que necesariamente $BG \cap AE = F$, $DC \cap AE = F$, $DG \cap AE = E$.

Así vemos que existe un plano de orden 2 salvo isomorfismo (el plano de Fano).

1.1. Colineaciones

Como los puntos y las rectas son los elementos básicos de un plano proyectivo las funciones que nos van a interesar son aquellas que envían puntos en puntos y rectas en rectas.

Definición. 1.10. Una *colineación* \mathcal{C} en un plano proyectivo es una función biyectiva del conjunto de puntos a sí mismo que manda rectas en rectas.

Por ejemplo la identidad es una colineación. En el plano de Fano vemos que intercambiar las rectas AB y BC a manera de reflexión produce una colineación (ver figura 1.5).

Proposición. 1.11. El conjunto de *colineaciones* de un plano proyectivo finito es un grupo con la composición.

Demostración. Sean \mathcal{C} y \mathcal{B} colineaciones de un plano Π . Tomamos una recta l en el plano, entonces $\mathcal{B}(l) = l'$ es una recta y $\mathcal{C}(l')$ es una recta por que \mathcal{C} es una colineación, por lo que $\mathcal{CB}(l)$ es una recta y el conjunto de colineaciones es cerrado bajo la

operación.

La función identidad es biyectiva y deja fijas a las rectas por lo tanto es una colineación.

Como las colineaciones son funciones biyectivas sus funciones inversas existen. Veamos que la inversa de una colineación manda rectas en rectas. Sea l una recta en un plano de orden k , entonces consta de $k + 1$ puntos y por lo tanto $\mathcal{C}^{-1}(l)$ también tiene $k + 1$ puntos. Supongamos que $\mathcal{C}^{-1}(l)$ no es una recta. Entonces existen tres puntos A, B, C en la preimagen que no son colineales. Sin embargo, las imágenes de las rectas AB, BC y CA bajo la colineación están en l . Lo anterior no es posible ya que su unión involucra más de $k + 1$ puntos. ■

Hay dos tipos de colineaciones de especial interés para nosotros: las centrales y las axiales.

Definición. 1.12. Una *colineación central* \mathcal{C} es una colineación tal que existe un punto P llamado *centro* que satisface lo siguiente:

- i) P es un punto fijo,
- ii) Para cada punto X se cumple que $\mathcal{C}(X) \in PX$.

La colineación de la figura 1.5 es una colineación central que tiene por centro al punto F .

Observación. 1.13. Sea X un punto en un plano proyectivo. Si tenemos una colineación central con centro P , la recta PX estará fija bajo la colineación, ya que cualquier punto A distinto de P en la recta PX es tal que $\mathcal{C}(A) \in PA = PX$. Por lo tanto cada colineación central induce una permutación en el conjunto de puntos en cada recta que pasa por P .

De forma dual definimos otro tipo de colineación.

Definición. 1.14. Una *colineación axial* es una colineación con una recta fija, a la que llamamos *eje*, que está fija punto por punto.

La colineación de la figura 1.5 además de ser una colineación central es una colineación axial que tiene por eje la recta BF .

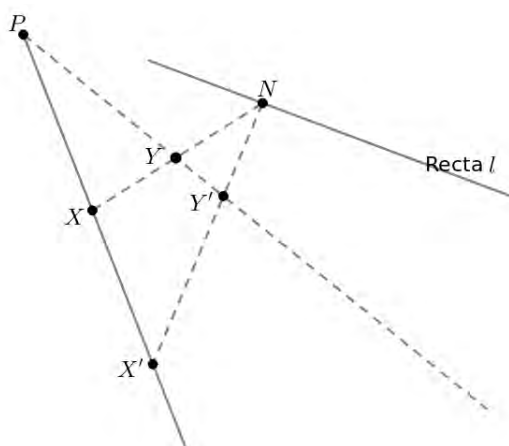


Figura 1.6:

En realidad las colineaciones centrales son axiales y las colineaciones axiales son centrales. Antes de verificar lo anterior notemos primero que:

Lema. 1.15. Una colineación central que tiene un eje está determinada de forma única por el centro P , por el eje l , un punto X que no pertenece a l , y la imagen de X .

Demostración. Sean \mathcal{C} una colineación central, sea $Y \notin XP$ tal que $Y \notin l$, y sea Y' la imagen de Y . Tenemos que $Y' \in PY$. Sea $N = XY \cap l$; la imagen de la recta XN es la recta $X'N$, entonces $Y' \in X'N$. Dado que también $Y' \in PY$, vemos que $Y' = X'N \cap PY$ (ver figura 1.6).

Sea Z un punto en XP diferente de X y de P , podemos encontrar su imagen de forma análoga. ■

Lema. 1.16. Sea \mathcal{C} una colineación central y l una recta que no queda invariante bajo \mathcal{C} , entonces $\mathcal{C}(l) \cap l$ es un punto fijo de \mathcal{C} .

Demostración. Sea $A = \mathcal{C}(l) \cap l$ y P el centro de la colineación. Tenemos que $\mathcal{C}(A) \in \mathcal{C}(l)$, y como es una colineación central, $\mathcal{C}(A) \in PA$. Por lo tanto $\mathcal{C}(A) = A$. ■

La colineación identidad es central y fija a todas las rectas punto por punto, por lo que todas las rectas son ejes. Para colineaciones centrales que no son la identidad tenemos la siguiente proposición.

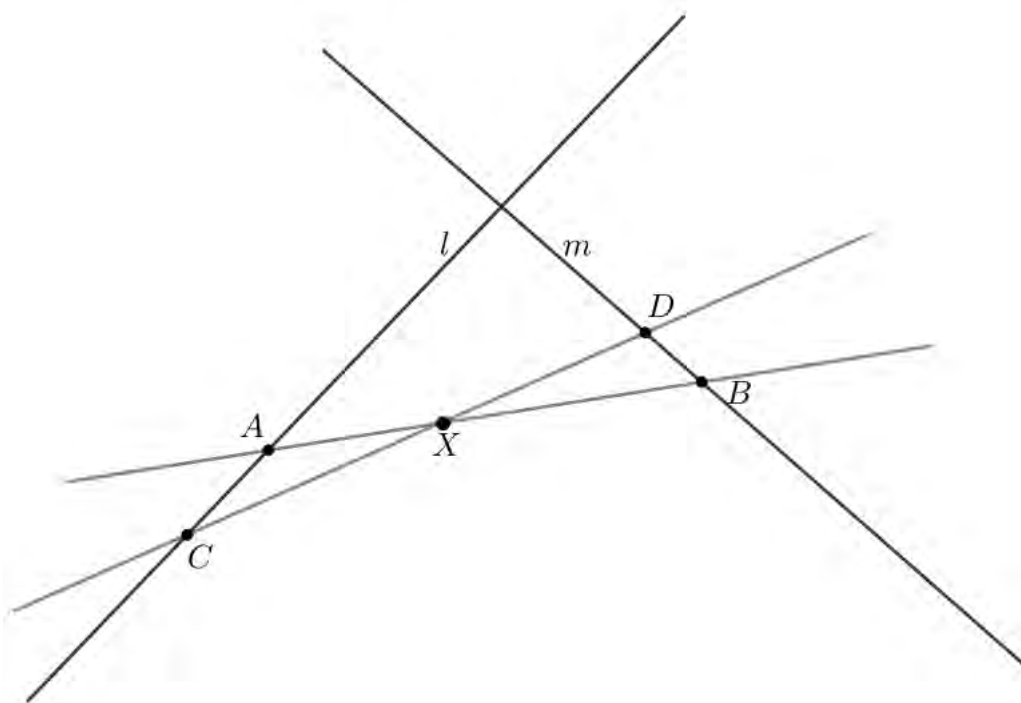


Figura 1.7:

Proposición. 1.17. Cada colineación central \mathcal{C} distinta de la identidad tiene un eje y es único.

Demostración. Supongamos que hay más de un eje, sean l y m ejes distintos. Sea X un punto tal que $X \neq P$, $X \notin l$ y $X \notin m$. Sean $A, C \in l$ tales que $A, C \notin m$ (ver figura 1.7). La recta AX intersecta a m en un punto B , de igual forma CX intersecta a m en un punto D distinto de B . Como l y m son ejes A, B, C y D son puntos fijos y las rectas AX y CX están fijas, por lo tanto X es fijo. Entonces todos los puntos están fijos y \mathcal{C} es la colineación identidad. Esto quiere decir que a lo más hay un eje en cada colineación central no trivial.

Ahora probemos la existencia de dicho eje bajo el supuesto de que hay una recta invariante que no pasa por el centro. Supongamos que hay una recta invariante l que no pasa por el centro P . Si A es un punto en l , PA es una recta invariante, entonces $\mathcal{C}(A) \in PA$ y $\mathcal{C}(A) \in l$, por lo que A es un punto fijo, y así l es un eje.

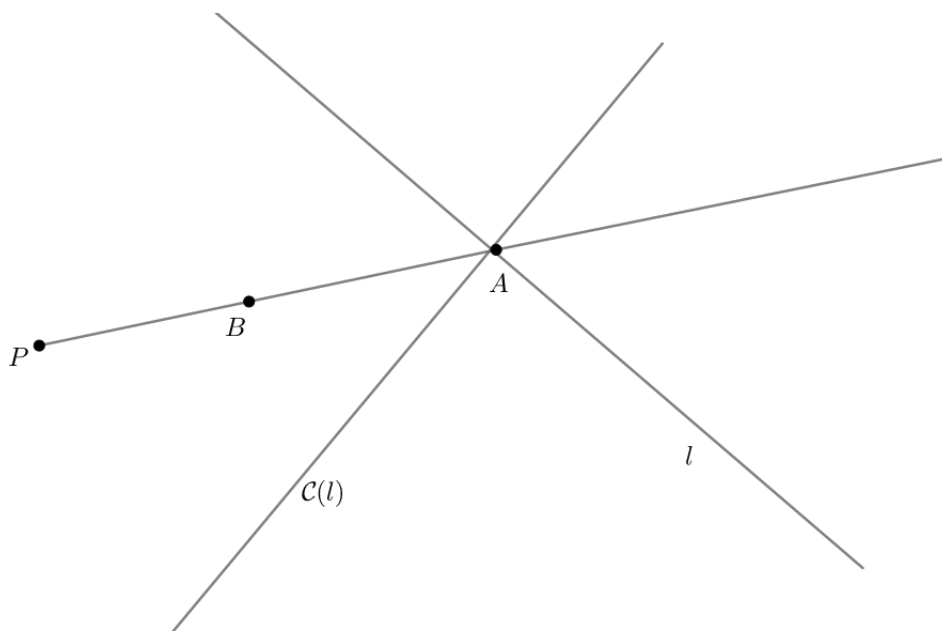


Figura 1.8:

Finalmente probamos la existencia. Tomemos una recta l que no pase por P . Si es invariante entonces es el eje. Si no, tomemos a $A = l \cap \mathcal{C}(l)$, y notemos que A es fijo por el lema 1.16 (ver figura 1.8). Si PA es fijo punto por punto, es el eje.

Si \mathcal{C} no fija a todos los puntos de PA , tomamos $B \in PA$ que no es fijo y tomamos una recta $m \neq PA$ que pasa por B (ver figura 1.9). La recta no es invariante pues de lo contrario su intersección con PA sería un punto fijo, pero esa intersección es B . Como vimos para A tenemos que $C = m \cap \mathcal{C}(m)$ es un punto fijo, de donde vemos que la recta AC es invariante y no pasa por P , por lo tanto es el eje. ■

También tenemos que toda colineación axial es central.

Proposición. 1.18. Toda colineación axial no trivial tiene uno y sólo un centro.

Demostración. Sea \mathcal{C} una colineación axial con eje l . Supongamos que P y P' son centros distintos y sea X un punto que no este en la recta PP' . Como P es centro, PX está fija y por lo mismo $P'X$ es fija. Entonces su intersección X es un punto fijo. De esta manera tenemos que todas las rectas están fijas, y por lo tanto los puntos también, así que es la colineación trivial.

Si hay un punto fijo P que no esté en l , cualquier recta m que pasa por P intersecta a l . Por lo tanto es una recta invariante, ya que tiene dos puntos fijos P y $m \cap l$.

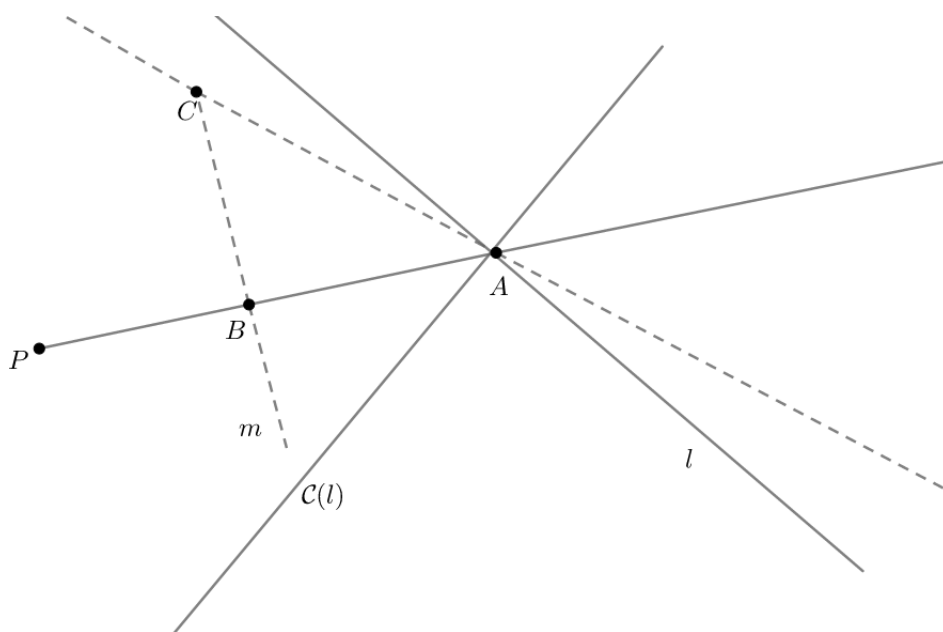


Figura 1.9:

Así que P es centro. Sólo resta analizar el caso en que no hay puntos fijos fuera de l . Sean $X, Y \notin l$ puntos distintos, sea P la intersección de $XC(X)$ y l , y P' la intersección de $YC(Y)$ y l . La intersección de $XP = C(X)P$ y $YP' = C(Y)P'$ es un punto fijo (ya que XP y YP' son rectas invariantes) así que está en l por que no hay puntos fijos fuera de l , por lo tanto $P = P'$. Entonces P es centro ya que es la intersección de las rectas $XC(X)$. ■

En adelante utilizaremos los siguientes nombre para las colineaciones centrales dependiendo de si el centro está o no en el eje.

Homología. Colineación central con centro y eje no incidentes. Una homología con centro P y eje l la denotamos como una (P, l) -homología.

Elación. Colineación central con centro y eje incidentes. Una elación con centro P y eje l la denotamos como una (P, l) -elación.

Por ejemplo, como vimos anteriormente en el plano de Fano intercambiar las rectas AB y BC a manera de reflexión produce una elación con centro F y eje BF (ver figura 1.5).

Una (P, l) -colineación, es un colineación central tal que P es el centro y l es el eje.

Recordemos que si \mathcal{C} es una (P, l) -colineación y X un punto distinto de P que no está en l , entonces $\mathcal{C}(X)$ pertenece a la recta PX . Dado cualquier punto $X' \in PX$ diferente de P , nos interesa saber si existe una (P, l) -colineación en la cual la imagen de X sea X' .

Un plano Π es (P, l) -transitivo si para cualesquiera puntos X, X' colineales con P tales que $X, X' \neq P$ y $X, X' \notin l$ hay una (P, l) -colineación que envía X a X' . A continuación veremos que la existencia de un punto P y una recta l para los cuales Π es (P, l) -transitivo puede implicar la existencia de otros puntos P' y rectas l' para las cuales Π sea (P', l') -transitivo.

Teorema. 1.19. Sean Π un plano proyectivo que es (P, l) -transitivo y τ una colineación de Π . Entonces Π es $(\tau(P), \tau(l))$ -transitivo.

Demostración. Sean Y, Y' puntos colineales con $P' := \tau(P)$ tales que $Y, Y' \notin \tau(l)$. Definimos $X = \tau^{-1}(Y)$ y $X' = \tau^{-1}(Y')$, sabemos que $X, X' \notin l$. Como τ^{-1} es también una colineación, X, X' y P son puntos colineales. Entonces, como Π es (P, l) -transitivo, existe una (P, l) -colineación A , tal que $A(X) = X'$. Mediante las colineaciones anteriores definimos $A' = \tau A \tau^{-1}$, tenemos que $A'(Y) = \tau A \tau^{-1}(Y) = \tau A(X) = \tau(X') = Y'$.

Hay que ver que A' es una $(\tau(P), \tau(l))$ -colineación. P' es punto fijo de A' ya que $\tau A \tau^{-1}(P') = \tau A(P) = \tau(P) = P'$. Además tenemos que $A'(Y) = \tau A \tau^{-1}(Y) = \tau A(X) = \tau(X') = Y'$, donde Y y Y' son los puntos definidos al inicio de esta demostración. Por lo tanto P' es centro de A' .

Por último veamos que la recta $\tau(l)$ es el eje. Sea $Z \in \tau(l)$, entonces $Z = \tau(L)$ con L un punto en el eje de la colineación A . De donde $A'(Z) = \tau A \tau^{-1}(Z) = \tau A(L) = \tau(L) = Z$. Por lo tanto $\tau(l)$ es el eje de la colineación A' . ■

Teorema. 1.20. Sea Π es un plano finito de orden n entonces:

- i) Si $P \in l$ y hay n (P, l) -elaciones distintas entonces Π es un plano (P, l) -transitivo.
- ii) Si $P \notin l$ y hay $n - 1$ (P, l) -homologías entonces Π es un plano (P, l) -transitivo.

Demostración. En el caso i) tomemos m una recta que pasa por P y $X \in m$ un punto distinto de P . Como hay n elaciones, cada elación manda a X a un punto distinto por el teorema 1.15. De manera análoga se prueba ii). ■

1.2. Planos desarguesianos

Examinemos una consecuencia interesante de tener una colineación central. Supongamos que τ es una colineación central no trivial con eje l y centro P . Sean X, Y, Z tres puntos tales que formen un cuadrángulo regular con P . Sean $\tau(X) = X', \tau(Y) = Y', \tau(Z) = Z'$. Como vimos en el lema 1.16, los puntos $A = XY \cap X'Y', B = YZ \cap Y'Z'$ y $C = ZX \cap Z'X'$ son puntos fijos diferentes de P . Esto quiere decir que los puntos A, B y C pertenecen a l ya que la colineación es no trivial (una colineación no trivial no tiene puntos fijos además de los puntos del eje y el centro, ver teorema 1.17).

Lo que acabamos de ver es que una colineación central nos da una configuración de puntos a la que llamamos *configuración de Desargues*. En esta configuración se tienen dos triángulos X, Y, Z y X', Y', Z' (un triángulo es un conjunto de 3 puntos no colineales) tales que las rectas XX', YY' y ZZ' concurren en un punto P , y que los puntos $XY \cap X'Y', YZ \cap Y'Z'$ y $ZX \cap Z'X'$ son colineales (ver figura 1.10). Decimos que dos triángulos X, Y, Z y X', Y', Z' están en *perspectiva* desde un punto P si PXX', PYY' y PZZ' son rectas.

Un plano proyectivo es *desarguesiano* si cualesquiera dos triángulos en perspectiva inducen una configuración de Desargues. Como vimos, las colineaciones centrales nos dan una configuración de Desargues y esto es fundamental para el siguiente teorema.

Teorema. 1.21. Un plano proyectivo Π es desarguesiano si es (P, l) -transitivo para cualquier punto P y cualquier recta l .

Demostración. Sean XYZ y $X'Y'Z'$ dos triángulos en perspectiva desde P . Como el plano es (P, l) -transitivo para cualquier punto P y recta l . Existe una (P, YZ) -colineación \mathcal{C}_x que envía X a X' , una $(P, X'Z')$ -colineación \mathcal{C}_y que envía Y a Y' y una $(P, X'Y')$ -colineación \mathcal{C}_z con $\mathcal{C}(Z) = Z'$. Entonces $\mathcal{C} := \mathcal{C}_z\mathcal{C}_y\mathcal{C}_x$ cumple que es una colineación con centro P que satisface $\mathcal{C}(X) = X', \mathcal{C}(Y) = Y'$ y $\mathcal{C}(Z) = Z'$. Por la discusión anterior concluimos $XY \cap X'Y', YZ \cap Y'Z'$ y $ZX \cap Z'X'$ son colineales. ■

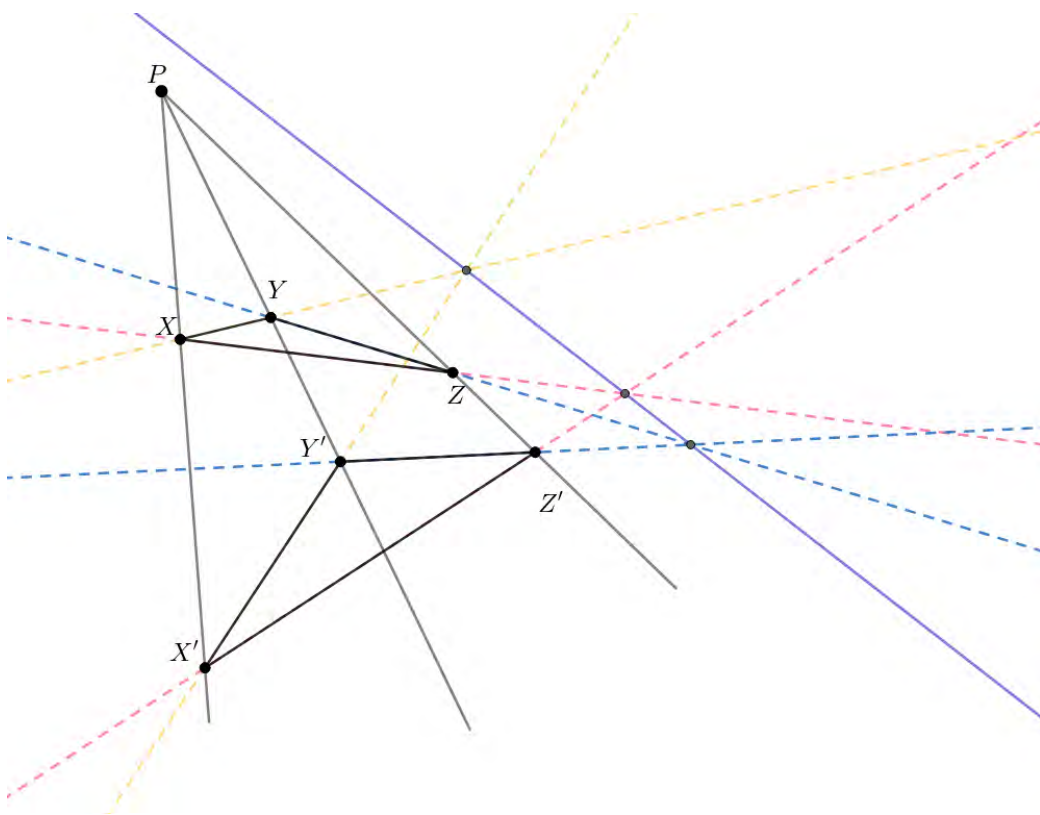


Figura 1.10: Configuración de Desargues

Capítulo 2

Planos proyectivos sobre campos

Dado K un campo construiremos un plano proyectivo $\Pi(K)$ sobre K . Los puntos son las clases de ternas ordenadas de $K^3 := \{(x, y, z) : x, y, z \in K\}$ diferentes de $(0, 0, 0)$ bajo la relación de equivalencia $(x, y, z) = (x, y, z)h$ para todo $h \in K \setminus 0$.

Una recta del plano proyectivo $\Pi(K)$ sobre K es el conjunto de puntos que satisfacen una ecuación $ax + by + cz = 0$, donde $a, b, c \in K$. Si un punto (x_0, y_0, z_0) satisface la ecuación de una recta $ax + by + cz = 0$, tenemos que $ax_0 + by_0 + cz_0 = 0$ de donde vemos que se cumple que $ax_0h + by_0h + cz_0h = 0$, por lo que cualquier representante de un punto cumple la ecuación.

Notemos que $(ka)x + (kb)y + (kc)z = 0$ con $k \neq 0$ representa la misma recta que $ax + by + cz = 0$.

Teorema. 2.1. Cada campo K determina un plano proyectivo $\Pi(K)$.

Demostración. Primero veamos que por cualesquiera dos puntos pasa una recta. Dos puntos diferentes (x_1, y_1, z_1) y (x_2, y_2, z_2) están en una recta si y sólo si para algunos $a, b, c \in K$:

$$ax_1 + by_1 + cz_1 = 0, \tag{2.1}$$

$$ax_2 + by_2 + cz_2 = 0. \tag{2.2}$$

Para la existencia de dicha recta basta que el sistema de ecuaciones dado por las ecuaciones 2.1 y 2.2 tenga solución, lo cual es inmediato ya que K es un campo. Con esto probamos que por cualesquiera dos puntos pasa una única recta.

Tenemos que dos rectas $a_1x + b_1y + c_1z = 0$ y $a_2x + b_2y + c_2z = 0$ se intersectan en un único punto (x', y', z') si y sólo si

$$a_1x' + b_1y' + c_1z' = 0, \quad (2.3)$$

$$a_2x' + b_2y' + c_2z' = 0. \quad (2.4)$$

Como el rango de la matriz asociada al sistema es 2, el sistema como solución a subespacio de dimensión 1, que representa al punto de $\Pi(K)$ que pertenece a las dos rectas.

Por último para concluir la prueba falta ver la existencia de un cuadrángulo regular. Afirmamos que los puntos $\{ (1, 1, 1), (1, 0, 0), (0, 1, 0), (0, 0, 1) \}$ cumplen que son un cuadrángulo regular, es decir no hay 3 que sean colineales.

Una recta que pase por los puntos $(1, 0, 0), (0, 1, 0)$ y $(0, 0, 1)$ cumple que:

$$a(1) + b(0) + c(0) = 0,$$

$$a(0) + b(1) + c(0) = 0,$$

$$a(0) + b(0) + c(1) = 0,$$

pero esto implica que $a = b = c = 0$.

Una recta que pase por los puntos $(1, 1, 1), (1, 0, 0), (0, 1, 0)$ debe cumplir que

$$a(1) + b(1) + c(1) = 0,$$

$$a(1) + b(0) + c(0) = 0,$$

$$a(0) + b(1) + c(0) = 0,$$

de donde vemos que $a = b = c = 0$. En los casos restantes se verifica como el último caso que $a = b = c = 0$. Por lo tanto no hay recta que pase por tres puntos $(1, 1, 1), (1, 0, 0), (0, 1, 0)$ y $(0, 0, 1)$. ■

De manera similar a las combinaciones lineales de K^3 , dados dos puntos $u = (x_1, y_1, z_1)$ y $v = (x_2, y_2, z_2)$ una *combinación lineal* de ellos es un punto $u\lambda + v\kappa = (x_1\lambda + x_2\kappa, y_1\lambda + y_2\kappa, z_1\lambda + z_2\kappa)$ con $\lambda, \kappa \in K$. Notemos que podemos obtener diferentes combinaciones para valores iguales de λ y κ si tomamos diferentes representantes de u y v .

Teorema. 2.2. Los puntos del plano proyectivo $\Pi(K)$ que están en la recta que pasa por los puntos u y v son combinaciones lineales de u y v . Además cualquier combinación lineal de u y v está en la recta que pasa por u y por v .

Demostración. Una combinación lineal de $u = (x_1, y_1, z_1)$ y $v = (x_2, y_2, z_2)$ es un punto $u\lambda + v\rho = (x_1\lambda + x_2\rho, y_1\lambda + y_2\rho, z_1\lambda + z_2\rho)$ con $\lambda, \rho \in K$, así que

$$\begin{aligned} & a(x_1\lambda + x_2\rho) + b(y_1\lambda + y_2\rho) + c(z_1\lambda + z_2\rho) \\ &= a(x_1\lambda) + b(y_1\lambda) + c(z_1\lambda) + a(x_2\rho) + b(y_2\rho) + c(z_2\rho) = 0. \end{aligned}$$

De lo anterior vemos que cualquier combinación lineal de u y v pertenece a la recta que pasa por estos dos puntos.

La ecuación de una recta de Π es la ecuación de un plano Σ (un subespacio de orden 2) en K^3 . De aquí se sigue que los puntos u y v pueden representarse como dos vectores u' y v' linealmente independientes de Σ , y por lo tanto generan a Σ . Sabemos que cualquier vector en Σ es combinación lineal de u' y v' . De aquí se sigue que todo punto de la recta de $\Pi(K)$ es combinación lineal de los puntos u y v . ■

2.1. Projectividades de $\Pi(K)$

Una *colineación proyectiva* es una colineación que es un producto finito de colineaciones centrales. El conjunto de colineaciones proyectivas de un plano proyectivo es un subgrupo del grupo de colineaciones y lo llamamos el grupo de proyectividades.

En un plano proyectivo sobre un campo tenemos que se cumple el siguiente criterio.

Lema. 2.3. Tres puntos en $\Pi(K)$ son colineales si y sólo si la matriz que tiene por columnas a las los vectores de coordenadas de los puntos es singular.

Demostración. Tres puntos x_1, x_2, x_3 son colineales si y sólo si x_3 es combinación lineal de x_1 y x_2 por el teorema 2.2, lo cual es equivalente a $x_3 = x_1h + x_2k$ para algunos $h, k \in K$ no ambos 0. Por lo tanto la matriz que tiene a estos puntos como columnas es singular. Por otro lado, si la matriz es singular entonces una columna

es combinación lineal de las otras dos, así que un punto sera combinación lineal de los otros dos. ■

Podemos ver algunas colineaciones fácilmente como multiplicar por una matriz de 3×3 no singular con coordenadas en K .

Lema. 2.4. En un plano sobre un campo $\Pi(K)$ una matriz invertible de orden 3×3 con entradas en el campo define una colineación.

Demostración. Sea $ax + by + cz = 0$ una recta. Escribamos el vector que la representa como $[a, b, c]$. Sean M una matriz invertible de 3×3 con entradas en el campo y $\bar{x} = (x, y, z)$ un punto arbitrario en la recta. Tenemos que el producto punto de los vectores que representan a la recta y el punto es igual a 0, de modo que la ecuación se puede reescribir como

$$[a, b, c] \cdot (x, y, z) = 0. \quad (2.5)$$

Como la inversa de M existe, podemos expresar la ecuación (2.5) de manera matricial como

$$\begin{pmatrix} a & b & c \end{pmatrix} M^{-1} M \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0,$$

así que el punto $M\bar{x}^T$ está en la recta $[a, b, c]M^{-1}$. Esta nueva recta no depende de la elección de (x, y, z) , por lo que todos los puntos que se obtienen de una recta al multiplicarlos por M están en la misma recta. Por lo tanto M es una colineación. ■

Examinemos primero las colineaciones de la forma:

$$M_1 = \begin{pmatrix} r & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

con r diferente de 0 y 1. Notemos que si $r = 0$ tendremos una matriz singular, y si $r = 1$ tendríamos a la matriz identidad, que corresponde a la colineación trivial.

Veamos que estas matrices representan colineaciones centrales no triviales (si $r \neq 0, 1$).

Sea $X = (x, y, z)$; entonces $AX = (rx, y, z)$. Denotemos por P_1 al punto $(1, 0, 0)$; afirmamos que éste será el centro de la colineación. Notemos primero que $AP_1 = (r, 0, 0) = (1, 0, 0)$, de modo que este punto está fijo. Por el lema 2.3, vemos que como

$$\det \begin{pmatrix} 1 & x & rx \\ 0 & y & y \\ 0 & z & z \end{pmatrix} = 0,$$

los puntos P_1, X y AX son colineales; de donde se deduce que P_1 es el centro. Además podemos ver que cada punto en la recta $x = 0$ está fijo ya que es de la forma $(0, y, z)$ y su imagen es el mismo, así que esta recta es el eje. Denotemos a la recta $x = 0$ por l_1 , y concluimos que la función anterior es una (P_1, l_1) -colineación.

De la misma forma procedemos para probar que la matriz

$$M_2 := \begin{pmatrix} 1 & s & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

con $s \neq 0$ es una colineación central con centro $P_1 = (1, 0, 0)$ y eje l_2 , que es la recta $y = 0$.

Veamos que P_1 es el centro. Para ello notemos que $AP_1 = (1, 0, 0)$, por lo que es un punto fijo. Veamos que deja invariantes a las rectas que pasan por él. Si $x = (x, y, z)$ es un punto cualquiera, su imagen es $Ax = (x + sy, y, z)$. Usando el criterio del lema 2.3 vemos que

$$\det \begin{pmatrix} 1 & x & x + cy \\ 0 & y & y \\ 0 & z & z \end{pmatrix} = 0,$$

y concluimos que los puntos son colineales, por lo que se prueba que P_1 es centro.

Un punto cualquiera de la recta l_2 es de la forma $(x, 0, z)$, y su imagen es $(x, 0, z)$, por lo que los puntos de l_2 quedan fijos. Como la multiplicación por M_2 no es la función identidad, l_2 es el único eje. Así probamos que M_2 es una (P_1, l_2) -colineación no trivial.

En adelante denotaremos

$$\begin{aligned} P_1 &= (1, 0, 0), \\ l_1 &\text{ la recta } x = 0, \\ l_2 &\text{ la recta } y = 0. \end{aligned} \tag{2.6}$$

Proposición. 2.5. El plano $\Pi(K)$ es (P_1, l_1) -transitivo y (P_1, l_2) -transitivo para P_1, l_1 y l_2 descritos en (2.6).

Demostración. Como vimos anteriormente las colineaciones dadas por la matrices

$$\begin{pmatrix} \mu & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ con } \mu \in \mathcal{Q} \setminus \{0\},$$

son (P_1, l_1) -colineaciones. Así que $\Pi(K)$ es (P_1, l_1) -transitivo por el teorema 1.20, ya que hay ocho (P_1, l_1) -colineaciones distintas, una por cada $\mu \in \mathcal{Q} \setminus \{0\}$.

Por otro lado, hemos visto que las colineaciones dadas por la matrices

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

con $\nu \in \mathcal{Q}$, inducen (P_1, l_2) -colineaciones. Por el teorema 1.21 concluimos que $\Pi(K)$ es (P_1, l_2) -transitivo ya que hay 9 colineaciones distintas de este tipo. ■

Los plano proyectivos sobre campos comparten algunas propiedades. Una de ellas es que son desarguesianos, como mostramos a continuación.

Teorema. 2.6. Todo plano proyectivo $\Pi(K)$ sobre un campo es desarguesiano.

Demostración. Sean P un punto y l una recta, veamos que $\Pi(K)$ es (P, l) -transitivo. Supongamos primero que $P \notin l$. Como K es un campo, la propiedad universal de las bases garantiza la existencia de una función \mathcal{C}_1 que manda $P_1 = (1, 0, 0)$ en P y $(0, 1, 0), (0, 0, 1)$ a dos puntos diferentes de l . La función \mathcal{C}_1 es una colineación (ver el lema 2.4). Tenemos que \mathcal{C}_1 manda P_1 a P y a l_2 a l , por lo que $\Pi(K)$ es (P, l) -transitivo como se prueba en el teorema 1.19.

Ahora consideremos el caso en que $P \in l$. Tomemos un punto $Q \in l$ distinto de P y un punto R que no está en l . Tenemos una colineación \mathcal{C}_2 , que se obtiene de mandar $(1, 0, 0)$ a P , $(0, 0, 1)$ a Q y $(0, 1, 0)$ a R . Como $\Pi(K)$ es (P_1, l_2) -transitivo, y \mathcal{C}_2 manda a P_1 en P y l_2 en l , entonces $\Pi(K)$ también es (P, l) -transitivo por el teorema 1.19.

Como para cualquier punto P y cualquier recta l se tiene que $\Pi(K)$ es (P, l) -transitivo, por el lema 1.21 se deduce que es desarguesiano. ■

2.2. Otra construcción de $\Pi(K)$

Ya vimos que $\Pi(K)$ es un plano proyectivo si K es un campo. Podemos dar otra construcción para estos planos proyectivos de la siguiente manera; tomemos por puntos a las parejas ordenadas de $K^2 = \{(x, y) : x, y \in K\}$ y por rectas a los subconjuntos que cumplen alguna de la siguientes ecuaciones.

$$y = xm + k, \tag{2.7}$$

$$x = c, \tag{2.8}$$

con $m, k, c \in K$.

Es fácil verificar que por cualesquiera dos puntos pasa una recta resolviendo un sistema de ecuaciones, sin embargo hay rectas que no se intersectan. Dos rectas $y = mx + k_1$ y $y = mx + k_2$ no se intersectan si $k_1 \neq k_2$, y las rectas $x = c_1$ y $x = c_2$ con $c_1 \neq c_2$ no se intersectan (notemos que el ser paralelo es un relación de equivalencia, así que podemos hacer una partición del conjunto de rectas en clases

de paralelas). Agregamos una recta con puntos de intersección para cada clase de rectas paralelas, esta recta la llamamos la recta ideal.

Veamos que los puntos $(x, y, 1)$ de $\Pi(K)$ se corresponden con los puntos (x, y) de K^2 , las rectas $ax + by + cz = 0$ de $\Pi(K)$ se corresponden con las rectas $ax + by = c$ de K^2 . La recta $z = 0$ se corresponde con la recta ideal. Por lo que basta agregar la recta ideal a K^2 para obtener un plano proyectivo isomorfo a $\Pi(K)$.

Capítulo 3

Casi-campos de 9 elementos.

Los campos finitos son parte de un concepto más amplio, que son los casi-campos. Los minicuaternios son un casi-campo como veremos más adelante.

Definición. 3.1. Un casi-campo es un conjunto S con dos operaciones binarias $+$ y \bullet que cumple las siguientes propiedades.

- S es finito,
- $(S, +)$ es un grupo abeliano con neutro 0 ,
- $(S \setminus \{0\}, \bullet)$ es un grupo con 1 como neutro,
- \bullet es distributiva por la derecha respecto a $+$, es decir, $(\mu + \sigma) \bullet \lambda = (\mu \bullet \lambda) + (\sigma \bullet \lambda)$ para todo $\sigma, \mu, \lambda \in S$,
- $\mu \bullet 0 = 0$ para todo $\mu \in S$.

Todo campo es un casi-campo en que las dos leyes distributivas se cumplen.

Como es usual, en la expresión $\mu \bullet \sigma$ omitiremos \bullet y escribiremos simplemente $\mu\sigma$.

de un casi-campo se define como la cardinalidad del conjunto de elementos.

Algunas propiedades de los campos se satisfacen en todo casi-campo. A continuación veremos alguna de estas propiedades.

Proposición. 3.2. Para toda μ en un casi-campo se satisface $0 \bullet \mu = 0$.

Demostración. $0 \bullet \mu = (0 + 0) \bullet \mu = 0 \bullet \mu + 0 \bullet \mu$ de donde $0 \bullet \mu = 0$. ■

Proposición. 3.3. Si $\mu \bullet \sigma = 0$ entonces $\mu = 0$ ó $\sigma = 0$.

Demostración. Supongamos que $\sigma \neq 0$, entonces

$$0 = \mu \bullet \sigma \bullet \sigma^{-1} = \mu \bullet 1 = \mu.$$

De manera análoga si $\mu \neq 0$ vemos que $\sigma = 0$. ■

En este trabajo centraremos nuestro estudio a los casi-campos finitos de orden 9. Dado cualquier casi-campo finito de orden 9, el conjunto $\mathcal{D} := \{0, 1, -1\}$ juega un rol especial. El subgrupo de $(\mathcal{S}, +)$ generado por 1 contiene a 0 y -1 . Tenemos que $1 \neq -1$, o de lo contrario $0 = 1 - 1 = 1 + 1$, y entonces el subgrupo generado por 1 sería de orden 2, pero $2 \nmid 9$ lo cual contradice el teorema de Lagrange. Como el grupo aditivo tiene orden 9,

$$(1 + 1 + 1)(1 + 1 + 1) = 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 = 0,$$

así por la proposición 3.3 tenemos que $1 + 1 + 1 = 0$. Entonces el subgrupo generado por 1 tienen orden 3 por lo que es \mathcal{D} . Para conocer el producto de cualquier par de elementos de \mathcal{D} sólo falta ver $-1 \bullet -1 = (1 + 1) \bullet -1 = 1(-1) + 1(-1) = -1 - 1 = 1$. Así vemos que $(\mathcal{D}, +, \bullet)$ es el campo de orden 3.

En cualquier casi-campo de orden 9 se cumple lo siguiente.

Observación. 3.4. Sea \mathcal{S} un casi-campo finito de orden 9. Supongamos que $\mu \in \mathcal{S}$ y $\mu \notin \mathcal{D}$. Entonces cada elemento de \mathcal{S} se puede escribir de manera única como $a + b \bullet \mu$ para algunas $a, b \in \mathcal{D}$.

Demostración. Para verificar lo anterior supongamos primero que $a + b\mu = a' + b'\mu$, entonces

$$a - a' = b'\mu - b\mu = (b' - b)\mu.$$

Si $b' \neq b$, entonces $(b' - b)^{-1} \bullet (a - a') = (b' - b)^{-1} \bullet (b' - b) \bullet \mu = \mu \in \mathcal{D}$, pero $\mu \notin \mathcal{D}$. Por lo tanto $b' = b$ y entonces $a' = a$. Hay 9 elementos diferentes de la forma $a + b\mu$, así que son los 9 elementos de \mathcal{S} . ■

Esto nos da una correspondencia biyectiva entre los elementos del casi-campo (escritos de la forma $a + b\mu$) y las parejas ordenadas (a, b) con entradas en \mathcal{D} . La suma de dos elementos $a + b\mu$ y $a' + b'\mu$, nos da $a + b\mu + a' + b'\mu = a + a' + (b + b')\mu$ y entonces podemos definir la suma en la forma $(a, b) + (a', b') = (a + a', b + b')$. Por lo tanto, la suma está determinada por los elementos de \mathcal{D} . Así que la suma en cualquier casi campo de orden 9 se define de la misma manera.

Observación. 3.5. La suma de parejas ordenadas de elementos de \mathcal{D} definida en el párrafo anterior induce un grupo aditivo.

A continuación probaremos algunas propiedades que cumplen los casi campos de orden 9.

Lema. 3.6. Sea \mathcal{R} un casi campo finito de orden 9, entonces para todo $\mu, \sigma \in \mathcal{R}$ tenemos que:

- I) $\mu + \mu + \mu = 0$.
- II) $(-1) \bullet \mu = -\mu = \mu \bullet (-1)$.
- III) $(-\mu) \bullet \sigma = -\mu \bullet \sigma = \mu \bullet (-\sigma)$.
- IV) $(-\mu) \bullet (-\sigma) = \mu \bullet \sigma$.

Demostración. I) $\mu + \mu + \mu = (1 + 1 + 1) \bullet \mu = 0 \bullet \mu = 0$.

II) Por el inciso anterior, $\mu + \mu = -\mu$. Entonces $(-1)\mu = (1 + 1)\mu = \mu + \mu = -\mu$. Ahora veamos que $\mu(-1) = (-1)\mu$. Si $\mu \in \mathcal{D}$ el enunciado se cumple ya que 1 y 0 conmutan con cualquier elemento y -1 conmuta consigo mismo. Ahora supongamos que $\mu \notin \mathcal{D}$. Tenemos 6 elementos que no están en \mathcal{D} ; digamos η, ν, λ y sus inversos aditivos, todos elementos distintos. Procederemos por reducción al absurdo suponiendo que $\eta(-1) \neq -\eta$, entonces sin pérdida de generalidad $\eta(-1) = \nu$. Así tenemos que

$$-\eta(-1) = -\nu,$$

$$\nu(-1) = \eta(-1)(-1) = \eta,$$

$$-\nu(-1) = -\eta.$$

De aquí se sigue que $\lambda(-1)$ tiene que ser igual a $-\lambda$; por lo que al menos hay un elemento tal que $\mu(-1) = -1$. Por la observación 3.4 cualquier elemento puede ser escrito de la forma $a + b\lambda$. Así,

$$(a + b\lambda)(-1) = a(-1) + b\lambda(-1) = -a + b(-\lambda) = -a + b(-1\lambda) = -a - b\lambda = -(a + b\lambda).$$

Lo que contradice que $\eta(-1) \neq -\eta$, por lo que -1 conmuta con todos los elementos del casi-campo.

Veamos que III) se cumple. Usando II) sabemos que

$$(-\mu) \bullet \sigma = (-1) \bullet \mu \bullet \sigma = -\mu \bullet \sigma = \mu \bullet \sigma(-1) = \mu \bullet -\sigma.$$

Por último verifiquemos el inciso IV)

$$(-\mu) \bullet (-\sigma) = (-1)\mu(-1) \bullet \sigma = (-1)(-1)\mu \bullet \sigma = \mu \bullet \sigma.$$

■

3.1. El campo de orden 9

Construiremos un casi-campo de orden 9 al que llamaremos \mathcal{F} ; éste resulta ser el campo de 9 elementos. Tomamos las parejas ordenadas (a, b) con $a, b \in \mathcal{D}$. Definimos la suma y el producto de la siguiente manera:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),$$

$$(a_1, b_1) \times (a_2, b_2) = (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1).$$

Por la observación 3.5 tenemos que el conjunto $\mathcal{F} = \{(a, b) : a, b \in \mathcal{D}\}$ con la operación $+$ forma un grupo conmutativo; donde la identidad es $(0, 0)$ y el inverso de (a, b) es $(-a, -b)$. De igual forma $\mathcal{F} \setminus \{(0, 0)\}$ con la operación \times es un grupo conmutativo, con elemento neutro $(1, 0)$ e inversos dados por $(a, b)^{-1} = (a(a^2 + b^2)^{-1}, -b(a^2 + b^2)^{-1})$. Las pruebas de conmutatividad, asociatividad, distributividad e inversos son análogas a las de los números complejos.

Escribimos $(a, 0) = a$ y $(0, 1) = \epsilon$. Así podemos escribir a cada elemento (a, b) como $a + b\epsilon$ con $\epsilon^2 = -1$, por lo que $\epsilon^4 = (1, 0) = 1$. El grupo multiplicativo es un

+	1	ω	ω^2	ω^3	ω^4	ω^5	ω^6	ω^7
1	ω^4	ω^7	ω^3	ω^5	0	ω^2	ω	ω^6
ω	ω^7	ω^5	1	ω^4	ω^6	0	ω^3	ω^2
ω^2	ω^3	1	ω^6	ω	ω^5	ω^7	0	ω^4
ω^3	ω^5	ω^4	ω	ω^7	ω^2	ω^6	1	0
ω^4	0	ω^6	ω^5	ω^2	1	ω^3	ω^7	ω
ω^5	ω^2	0	ω^7	ω^6	ω^3	ω	ω^4	1
ω^6	ω	ω^3	0	1	ω^7	ω^4	ω^2	ω^5
ω^7	ω^6	ω^2	ω^4	0	ω	1	ω^5	ω^3

Cuadro 3.1: Tabla de la operación + en términos de ω

grupo cíclico generado por $(1 - \epsilon)$. Vemos que las potencias 2, 4, 8 de $(1 - \epsilon)$ son $(1 - \epsilon)^2 = 1 + \epsilon + \epsilon^2 = \epsilon$, $(1 - \epsilon)^4 = \epsilon^2 = -1$, $(1 - \epsilon)^8 = 1$, y ninguna potencia menor a 8 es igual a 1. Denotamos $\omega = 1 - \epsilon$. Sus potencias son:

$$\begin{aligned} \omega &= 1 - \epsilon, & \omega^2 &= \epsilon, & \omega^3 &= 1 + \epsilon^3, & \omega^4 &= -1, \\ \omega^5 &= -1 + \epsilon, & \omega^6 &= -\epsilon, & \omega^7 &= -1 - \epsilon, & \omega^8 &= 1. \end{aligned}$$

Ver a los elementos de \mathcal{F} como potencias de ω simplifica la multiplicación, pero en cambio dificulta la suma. Sin embargo tenemos la relación $\omega^2 = -\omega + 1$, que nos ayuda a obtener la tabla 3.1.

Por último veamos que se cumple la siguiente igualdad que nos será útil más adelante.

Lema. 3.7. Sean $\omega^n, \omega^m \in \mathcal{F}$; entonces $(\omega^n + \omega^m)^3 = \omega^{3n} + \omega^{3m}$.

Demostración. Dado que el producto en \mathcal{F} es conmutativo sabemos que $(\omega^n + \omega^m)^3 = \omega^{3n} + 3\omega^{2n+m} + 3\omega^{n+2m} + \omega^{3m}$, donde $3\omega^r$ significa sumar 3 veces el elemento ω^r . Tenemos que en los casi-campos de 9 elementos, $3\omega^{2n+m} = 3\omega^{n+2m} = 0$ por inciso I) del lema 3.6 y esto prueba la igualdad. ■

3.2. minicuaternios \mathcal{Q}

Ya construimos un casi-campo de orden 9 que distribuye por la izquierda a la suma y es conmutativo. Ahora construiremos un sistema que no distribuye por la izquierda al cual llamaremos los minicuaternios y los denotaremos por \mathcal{Q} .

Los elementos de \mathcal{Q} son los mismos que los elementos de \mathcal{F} , es decir las 9 parejas $(a, b) = a + b\epsilon$. Como vimos anteriormente en la observación 3.5 la suma induce un grupo abeliano y todos los casi-campos de 9 elementos tienen la misma operación $+$ ya que depende de la suma de \mathcal{D} .

Para definir la multiplicación tomamos los siguientes conjuntos. $\mathcal{E} = \{1, \omega^2, \omega^4, \omega^6\}$, $\mathcal{O} = \{\omega, \omega^3, \omega^5, \omega^7\}$, con $\omega = 1 - \epsilon$. La nueva multiplicación \circ la definimos:

$$\omega^n \circ \omega^m = \begin{cases} \omega^n \times \omega^m = \omega^{n+m} & \text{si } \omega^m \in \mathcal{E}, \\ \omega^{3n} \times \omega^m = \omega^{3n+m} & \text{si } \omega^m \in \mathcal{O}, \end{cases}$$

(donde \times representa el producto en el campo).

Como habíamos dicho, el producto \circ no es conmutativo y no distribuye a la suma por la izquierda. Por ejemplo, $\omega^3 \circ \omega^2 = \omega^5$ y $\omega^2 \circ \omega^3 = \omega$ por lo que este producto no es conmutativo. Tenemos que $\omega \circ (\omega + 1) = \omega \circ \omega^7 = \omega^{3+7} = \omega^2$. Si la suma se distribuyera por la izquierda, $\omega \circ (\omega + 1)$ sería igual a $\omega \circ \omega + \omega \circ 1 = \omega^3 \omega^1 + \omega = \omega^4 + \omega$, pero esto último es igual a ω^6 .

Por la derecha veremos que sí distribuye a la suma y que se cumplirán las otras propiedades de un casi-campo.

Teorema. 3.8. \mathcal{Q} es un casi-campo con 9 elementos.

Demostración. Por definición \mathcal{Q} tiene 9 elementos y la suma $+$, por la observación 3.5, es una operación de grupo conmutativa. La operación \circ es operación de grupo para $\mathcal{Q} \setminus \{0\}$, tiene por neutro a $1 = \omega^0$ ya que $\omega^0 \circ \omega^n = \omega^n$ y $\omega^n \circ \omega^0 = \omega^n$ para toda n . Si $\omega^n \in \mathcal{E}$ entonces ω^n tiene por inverso a ω^{-n} , ya que $\omega^n \circ \omega^{-n} = \omega^{n-n} = \omega^{-n+n} = \omega^{-n} \circ \omega^n = 1$, y si $\omega^n \in \mathcal{O}$ entonces ω^n tiene por inverso a ω^{-3n} ya que $\omega^n \circ \omega^{-3n} = \omega^{3n-3n} = 1$ y $\omega^{-3n} \circ \omega^n = \omega^{-9n+n} = \omega^{-8n} = 1$.

Veamos que se cumple la distributividad por la derecha. Si $\omega^r \in \mathcal{E}$, entonces $(\omega^n + \omega^m) \circ \omega^r = (\omega^n + \omega^m) \times \omega^r = \omega^n \omega^r + \omega^m \omega^r = \omega^{n+r} + \omega^{m+r} = \omega^n \circ \omega^r + \omega^m \circ \omega^r$, y si $\omega^r \in \mathcal{O}$ entonces $(\omega^n + \omega^m) \circ \omega^r = (\omega^n + \omega^m) \times \omega^r = (\omega^{3n} + \omega^{3m}) \times \omega^r = \omega^{3n+r} + \omega^{3m+r} = \omega^n \circ \omega^r + \omega \circ \omega^r$.

Por último, se prueba la asociatividad de la siguiente manera. Si $\omega^m, \omega^r \in \mathcal{E}$, $(\omega^n \circ \omega^m) \circ \omega^r = \omega^{n+m} \circ \omega^r = \omega^{n+m+r}$. Como $\omega^{m+r} \in \mathcal{E}$, entonces $\omega^{n+m+r} = \omega^n \circ \omega^{m+r} = \omega^n \circ (\omega^m \circ \omega^r)$.

Si $\omega^m, \omega^r \in \mathcal{O}$, entonces $(\omega^n \circ \omega^m) \circ \omega^r = \omega^{3n+m} \circ \omega^r = \omega^{3(3n+m)+r} = \omega^{9n+3m+r}$. Como $\omega^{3m+r} \in \mathcal{E}$ y $\omega^{9n} = \omega^n$, entonces $\omega^{9n+3m+r} = \omega^n \circ \omega^{3m+r} = \omega^n \circ (\omega^m \circ \omega^r)$.

Si $\omega^r \in \mathcal{E}$ y $\omega^m \in \mathcal{O}$, entonces $(\omega^n \circ \omega^m) \circ \omega^r = \omega^{3n+m} \circ \omega^r = \omega^{3n+m+r}$. Como $\omega^{m+r} \in \mathcal{O}$, entonces $\omega^{3n+m+r} = \omega^n \circ \omega^{m+r} = \omega^n \circ (\omega^m \circ \omega^r)$.

Finalmente, si $\omega^r \in \mathcal{O}$ y $\omega^m \in \mathcal{E}$, entonces $(\omega^n \circ \omega^m) \circ \omega^r = \omega^{n+m} \circ \omega^r = \omega^{3n+3m+r}$. Como $\omega^{3m+r} \in \mathcal{O}$, entonces $\omega^{3n+3m+r} = \omega^n \circ \omega^{3m+r} = \omega^n \circ (\omega^m \circ \omega^r)$.

De lo anterior concluimos que \mathcal{Q} es un casi-campo con 9 elementos. ■

Observación. 3.9. Las potencias cuadradas de los elementos de \mathcal{Q} son:

$$\begin{aligned} 1 \circ 1 &= 1; & \omega \circ \omega &= \omega^4 = -1; & \omega^2 \circ \omega^2 &= \omega^4 = -1; & \omega^3 \circ \omega^3 &= \omega^4 = -1; \\ \omega^4 \circ \omega^4 &= 1; & \omega^5 \circ \omega^5 &= \omega^4 = -1; & \omega^6 \circ \omega^6 &= \omega^4 = -1; & \omega^7 \circ \omega^7 &= \omega^4 = -1. \end{aligned}$$

De la observación anterior vemos que -1 tiene 6 raíces cuadradas en \mathcal{Q} . Entonces el grupo multiplicativo de \mathcal{Q} es el grupo de los cuaternios. Tenemos que $\omega^4 = -1$ por lo cual, $\omega^5 = -\omega$, $\omega^6 = -\omega^2$ y $\omega^7 = -\omega^3$.

Así, por ejemplo, $\omega \circ \omega^2 = \omega^3$ y $\omega^2 \circ \omega = \omega^7 = -\omega^3$. Entonces tenemos que $\omega \circ \omega^2 = -\omega^2 \circ \omega = \omega^3$, de manera análoga $\omega \circ \omega^3 = -\omega^3 \circ \omega = -\omega^2$ y $\omega^2 \circ \omega^3 = -\omega^3 \circ \omega^2 = \omega$.

Ahora escribimos $\alpha = \omega$, $\beta = \omega^6$, $\gamma = \omega^7$. Con esta notación tenemos las siguientes igualdades:

$$\alpha \circ \beta = -\beta \circ \alpha = \gamma, \tag{3.1}$$

$$\beta \circ \gamma = -\gamma \circ \beta = \alpha, \quad (3.2)$$

$$\gamma \circ \alpha = -\alpha \circ \gamma = \beta, \quad (3.3)$$

$$\alpha \circ \alpha = \beta \circ \beta = \gamma \circ \gamma = -1. \quad (3.4)$$

Con estas igualdades podemos construir la tabla 3.3. Así tenemos que $\mathcal{Q} = \{0, \pm 1, \pm \alpha, \pm \beta, \pm \gamma\}$ y denotamos $\mathcal{Q}^* = \mathcal{Q} \setminus \mathcal{D}$.

Escribiremos simplemente los elementos seguidos para indicar la operación \circ cuando no se pueda confundir con la operación \times o alguna otra.

Teorema. 3.10. Las siguientes relaciones se cumplen en el casi-campo \mathcal{Q} :

- $\alpha - \beta = \beta - \gamma = \gamma - \alpha = 1,$
- $\alpha + \beta + \gamma = 0,$
- $\alpha^2 = \beta^2 = \gamma^2 = -1,$
- $\alpha\beta\gamma = -1,$
- $\beta\gamma = -\gamma\beta = \alpha,$
- $\gamma\alpha = -\alpha\gamma = \beta,$
- $\alpha\beta = -\beta\alpha = \gamma.$

Demostración. Recuerde que $\alpha = \omega$, $\beta = \omega^6$, $\gamma = \omega^7$, y que $-\alpha = \omega^5$, $-\beta = \omega^2$, $-\gamma = \omega^3$. De las tablas 3.2 y 3.3 se verifican las relaciones. ■

3.3. Automorfismos del casi campo de los mini-cuatrernios.

Sea $\sigma \in \mathcal{Q}^*$. Por la observación 3.4 tenemos que cualquier elemento de \mathcal{Q} se puede escribir como $a + b\sigma$ con $a, b \in \mathcal{D}$. Entonces la función que manda el elemento $a + b\alpha$ al elemento $a + b\sigma$ es una permutación de los elementos del casi-campo. Sea

+	1	α	$-\beta$	$-\gamma$	-1	$-\alpha$	β	γ
1	-1	γ	$-\gamma$	$-\alpha$	0	$-\beta$	α	β
α	γ	$-\alpha$	1	-1	β	0	$-\gamma$	$-\beta$
$-\beta$	$-\gamma$	1	β	α	$-\alpha$	γ	0	-1
$-\gamma$	$-\alpha$	-1	α	γ	$-\beta$	β	1	0
-1	0	β	$-\alpha$	$-\beta$	1	$-\gamma$	γ	α
$-\alpha$	$-\beta$	0	γ	β	$-\gamma$	α	-1	1
β	α	$-\gamma$	0	1	γ	-1	$-\beta$	$-\alpha$
γ	β	$-\beta$	-1	0	α	1	$-\alpha$	$-\gamma$

Cuadro 3.2: Tabla de la operación + en términos de α, β, γ .

\circ	1	α	$-\beta$	$-\gamma$	-1	$-\alpha$	β	γ
1	1	α	$-\beta$	$-\gamma$	-1	$-\alpha$	β	γ
α	α	-1	$-\gamma$	β	$-\alpha$	1	γ	$-\beta$
$-\beta$	$-\beta$	γ	-1	α	β	$-\gamma$	1	$-\alpha$
$-\gamma$	$-\gamma$	$-\beta$	$-\alpha$	-1	γ	β	α	1
-1	-1	$-\alpha$	β	γ	1	α	$-\beta$	$-\gamma$
$-\alpha$	$-\alpha$	1	γ	$-\beta$	α	-1	$-\gamma$	β
β	β	$-\gamma$	1	$-\alpha$	$-\beta$	γ	-1	α
γ	γ	β	α	1	$-\gamma$	$-\beta$	$-\alpha$	-1

Cuadro 3.3: Tabla de la operación \circ en términos de α, β, γ .

\mathcal{A} una de estas permutaciones, afirmamos que las siguientes propiedades se cumplen:

$$\mathcal{A}(\xi + \eta) = \mathcal{A}(\xi) + \mathcal{A}(\eta), \quad (3.5)$$

$$\mathcal{A}(\xi\eta) = \mathcal{A}(\xi)\mathcal{A}(\eta). \quad (3.6)$$

Primero verifiquemos (3.5). Sean $a + b\alpha$ y $a' + b'\alpha$ con $a, b, a', b' \in \mathcal{D}$. Aplicando \mathcal{A} a su suma obtenemos $\mathcal{A}(a + b\alpha + a' + b'\alpha) = \mathcal{A}(a + a' + (b + b')\alpha) = a + a' + (b + b')\sigma = a + b\sigma + a' + b'\sigma = \mathcal{A}(a + b\alpha) + \mathcal{A}(a' + b'\alpha)$.

El producto de dos elementos de \mathcal{Q} nos da otro elemento en el casi-campo, por lo que $(a + b\alpha)(a' + b'\alpha) = c + d\alpha$ para algunos $c, d \in \mathcal{D}$, que se obtienen a partir de los valores de a, a', b, b' y no dependen de α , eso se sigue de que el cuadrado de cualquier elemento en \mathcal{Q}^* es -1 . Entonces para cualquier otro elemento de $\sigma \in \mathcal{Q}$, tenemos que $(a + b\sigma)(a' + b'\sigma) = c + d\sigma$. Ahora, $\mathcal{A}((a + b\alpha)(a' + b'\alpha)) = \mathcal{A}(c + d\alpha) = c + d\sigma$ y $\mathcal{A}(a + b\alpha)\mathcal{A}(a' + b'\alpha) = (a + b\sigma)(a' + b'\sigma) = c + d\sigma$, lo que prueba (3.6).

Cualquier función de un casi-campo en sí mismo que cumpla las propiedades 3.5, 3.6 la llamaremos *automorfismo*. Las permutaciones mencionadas previamente cumplen con las propiedades 3.5 y 3.6, por lo tanto son automorfismos.

Teorema. 3.11. Los automorfismos del campo casi-campo \mathcal{Q} cumplen lo siguiente:

1. Son un grupo con la composición de funciones.
2. Cualquier automorfismo deja fijo a $0, 1$ y -1 .
3. Además de la identidad no hay automorfismos que dejen fijo a α .

Demostración. Sabemos que la composición de funciones es función. Si \mathcal{A} y \mathcal{B} son automorfismos entonces $\mathcal{B}\mathcal{A}(\xi + \eta) = \mathcal{B}(\mathcal{A}(\xi) + \mathcal{A}(\eta)) = (\mathcal{B}\mathcal{A})(\xi) + (\mathcal{B}\mathcal{A})(\eta)$.

De manera análoga para el producto, $\mathcal{B}\mathcal{A}(\xi\eta) = (\mathcal{B}\mathcal{A})(\xi)(\mathcal{B}\mathcal{A})(\eta)$. Esto prueba que la composición de automorfismos es un automorfismo.

La composición tiene por neutro a la función identidad, que trivialmente es un automorfismo.

Para probar el primer inciso resta verificar que el inverso de un automorfismo es un automorfismo. Sea \mathcal{A} un automorfismo y sean a, b dos elementos de \mathcal{Q} , entonces

hay dos elementos a', b' tales que $\mathcal{A}(a') = a$ y $\mathcal{A}(b') = b$. De aquí se sigue que $\mathcal{A}^{-1}(ab) = \mathcal{A}^{-1}(\mathcal{A}(a')\mathcal{A}(b')) = \mathcal{A}^{-1}(\mathcal{A}(a'b')) = a'b' = \mathcal{A}^{-1}(a')\mathcal{A}^{-1}(b')$. De manera análoga se prueba la propiedad 3.5.

Dado un automorfismo \mathcal{A} , tenemos que $\mathcal{A}(0) = \mathcal{A}(0+0) = \mathcal{A}(0) + \mathcal{A}(0)$. Así que $\mathcal{A}(0) = 0$.

De forma similar, tenemos que $\mathcal{A}(1) = \mathcal{A}(1 \circ 1) = \mathcal{A}(1) \circ \mathcal{A}(1)$ por lo que $\mathcal{A}(1) = 1$.

Por último $\mathcal{A}(1 + (-1)) = \mathcal{A}(1) + \mathcal{A}(-1) = 1 + \mathcal{A}(-1)$ y por otro lado $\mathcal{A}(1 + (-1)) = \mathcal{A}(0) = 0$, por lo que $\mathcal{A}(-1) = -1$.

Supongamos que existe un automorfismo \mathcal{A} tal que $\mathcal{A}(\alpha) = \alpha$. Entonces un elemento arbitrario $a + b\alpha$ tiene por imagen a $\mathcal{A}(a + b\alpha) = \mathcal{A}(a) + \mathcal{A}(b)\mathcal{A}(\alpha) = a + b\alpha$, por lo tanto es el automorfismo identidad. ■

Hasta ahora tenemos 6 automorfismos, que obtenemos de elegir a cualquiera de los seis elementos de \mathcal{Q}^* como la imagen de α .

Corolario. 3.12. Sólo hay 6 automorfismos de \mathcal{Q} .

Demostración. Supongamos que hay más. Entonces para algún $\rho \in \mathcal{Q}^*$ existen al menos dos automorfismos \mathcal{A} y \mathcal{B} que mandan α a ρ . Así, $\mathcal{B}^{-1}\mathcal{A}(\alpha) = \alpha$, pero por el teorema 3.11 debe ocurrir que $\mathcal{B}^{-1}\mathcal{A}$ es la identidad y por lo tanto $\mathcal{A} = \mathcal{B}$. ■

3.4. Soluciones de ecuaciones en \mathcal{Q}

Debido a que el casi-campo \mathcal{Q} no es conmutativo y no distribuye por la izquierda, encontrar soluciones para ecuaciones puede ser complicado incluso en el caso de las ecuaciones lineales.

Ya encontramos las soluciones de la ecuación $x^2 = -1$. La ecuación general lineal en \mathcal{Q} es de la forma

$$\rho x \rho' + \sigma x \sigma' = \tau$$

con todos los coeficientes distintos de cero. Usando la ley distributiva por la derecha obtenemos una ecuación equivalente

$$(\rho x \rho' (\sigma')^{-1} + \sigma x) \sigma' = \tau,$$

reescribiendo $\rho'(\sigma')^{-1}$ como ρ'' y $\tau(\sigma')^{-1}$ como τ'' tenemos que

$$\rho x \rho'' + \sigma x = \tau''.$$

Haciendo un cambio de variable con $y = \rho x$ y escribiendo $\sigma \rho^{-1} = \sigma''$, obtenemos la ecuación

$$y \rho'' + \sigma'' y = \tau''.$$

Entonces basta con solucionar ecuaciones de la forma:

$$x \rho + \sigma x = \tau.$$

Si $\rho \in \mathcal{D}$, tenemos que $x \rho = \rho x$ y entonces podemos usar la distributividad por la derecha para obtener $(\rho + \sigma)x = \tau$. Cuando $\rho + \sigma \neq 0$ la solución es

$$x = (\rho + \sigma)^{-1} \tau.$$

Y cuando $\rho + \sigma = 0$ la ecuación tiene solución si y sólo si $\tau = 0$, en cuyo caso cualquier elemento es solución.

El caso que nos va a interesar es en el que $\sigma = 1$, para este caso tenemos la ecuación

$$x \rho + x = \tau.$$

Ya vimos qué pasa cuando $\rho \in \mathcal{D}$, ahora suponemos que $\rho \in \mathcal{Q}^*$. Primero notemos que si \mathcal{A} es un automorfismo, entonces $\mathcal{A}(x)\mathcal{A}(\rho) + \mathcal{A}(x) = \mathcal{A}(\tau)$ si y sólo si $x\rho + x = \tau$. Si elegimos \mathcal{A} de manera que $\mathcal{A}(\rho) = \alpha$ y sustituimos $\mathcal{A}(x)$ por y y $\mathcal{A}(\tau)$ por τ' , tenemos la siguiente ecuación:

$$y\alpha + y = \tau'.$$

Con ayuda de las tablas 3.2 y 3.3 podemos dar valores a y y vemos que

$$y = 1, \quad y\alpha + y = \gamma; \quad y = -1, \quad y\alpha + y = -\gamma;$$

$$y = \alpha, \quad y\alpha + y = \beta; \quad y = -\alpha, \quad y\alpha + y = -\beta;$$

$$y = \beta, \quad y\alpha + y = 1; \quad y = -\beta, \quad y\alpha + y = -1;$$

$$y = \gamma, \quad y\alpha + y = -\alpha; \quad y = -\gamma, \quad y\alpha + y = \alpha;$$

$$y = 0, \quad y\alpha + y = 0.$$

De donde vemos que la ecuación tiene solución única para cada valor de τ' .

Teorema. 3.13. La ecuación $x\rho + x = \tau$ tiene una única solución si $\rho \neq -1$

Demostración. Si $\rho = 0$, entonces $x = \tau$. Si $\rho = 1$, entonces $\tau = x + x = -x$, así que $x = -\tau$. Por último, en caso de que $\rho \in \mathcal{D}^*$ tomemos un automorfismo \mathcal{A} tal que $\mathcal{A}(\rho) = \alpha$, por lo que tenemos una solución única μ para la ecuación $\mathcal{A}(x)\mathcal{A}(\rho) + \mathcal{A}(x) = \mathcal{A}(\tau)$. Entonces como $\mathcal{A}(x) = \mu$ y \mathcal{A} es un automorfismo; $x = \mathcal{A}^{-1}\mathcal{A}(x) = \mathcal{A}^{-1}(\mu)$. ■

Teorema. 3.14. Los siguientes sistemas de ecuaciones tienen solución única en \mathcal{Q} si $\mu \neq \mu'$:

$$y = \mu x + \kappa,$$

$$y = \mu' x + \kappa',$$

$$y = x\mu + \kappa,$$

$$y = x\mu' + \kappa'.$$

Demostración. Igualando el primer par de ecuaciones obtenemos $\mu x + \kappa = \mu' x + \kappa'$ y esto no da la ecuación

$$\kappa - \kappa' = \mu' x - \mu x = (\mu' - \mu)x$$

y por lo tanto $x = (\mu' - \mu)^{-1}(\kappa - \kappa')$.

Ahora igualando el segundo par de ecuaciones tenemos la ecuación $x\mu + \kappa = x\mu' + \kappa'$, a partir de la cual vemos que

$$\kappa - \kappa' = x\mu' - x\mu$$

la cual tiene solución única por el teorema 3.13. El valor de y lo obtenemos al sustituir el valor de x en cualquiera de las ecuaciones. ■

Capítulo 4

El plano Ω y Ω^D

En este capítulo construiremos un plano proyectivo Ω que tiene orden 9 sobre el casi-campo de los minicuaternios. A diferencia del plano de orden 9 que se obtiene a partir del campo con 9 elementos, el plano proyectivo que construiremos no es desarguesiano. También veremos que es diferente de su dual, el cual tampoco es desarguesiano. Así obtendremos 3 planos proyectivos diferentes de orden 9.

4.1. Construcción de Ω

Consideremos el conjunto de puntos $\Omega' = \{(x, y) : x, y \in \mathcal{Q}\}$ (81 puntos) y como rectas a los subconjuntos de puntos:

$$[\mu, \kappa] = \{(x, y) : y = x\mu + \kappa; \quad \mu, \kappa \in \mathcal{Q}\},$$

$$[\lambda] = \{(x, y) : x = \lambda; \quad \lambda \in \mathcal{Q}\}.$$

Hay 81 rectas $[\mu, \kappa]$ y 9 rectas $[\lambda]$. Llamaremos a μ la *pendiente* de la recta $y = x\mu + \kappa$.

Como veremos a continuación para cualesquiera dos puntos existe una recta que pasa por ellos, pero no todas las rectas se intersectan, así que Ω no es un plano proyectivo. Más adelante completaremos los puntos y la recta que nos faltan para obtener un plano proyectivo.

Lema. 4.1.

- Dos rectas $y = x\mu + \kappa_1$ y $y = x\mu + \kappa_2$ con $\mu, \kappa_1, \kappa_2 \in \mathcal{Q}$ y $\kappa_1 \neq \kappa_2$ no se intersectan.
- Cualesquiera dos rectas $x = \lambda_1$ y $x = \lambda_2$ con distintas $\lambda_1, \lambda_2 \in \mathcal{Q}$ no se intersectan.

Demostración. Si (x_0, y_0) es un punto en común para las rectas $y = x\mu + \kappa_1$ y $y = x\mu + \kappa_2$ entonces, $y_0 = x_0\mu + \kappa_1 = x_0\mu + \kappa_2$. Como $\kappa_1 \neq \kappa_2$, esto nos da una contradicción. Las rectas $x = \lambda$ consisten de los puntos (λ, y) por lo que dos rectas diferentes $x = \lambda_1$ y $x = \lambda_2$ no tienen puntos en común si $\lambda_1 \neq \lambda_2$. ■

Teorema. 4.2.

- Hay exactamente una recta que une dos puntos distintos de Ω .
- Dada una recta l y un punto P que no está en ella, existe una única recta que pasa por P y que no intersecta a l .

Demostración. Sean $A = (x_1, y_1)$ y $B = (x_2, y_2)$ puntos distintos. Si $x_1 = x_2$ entonces la recta $x = x_1$ contiene a los dos puntos. Además esta recta es única ya que si estuvieran en otra recta, se tendría que $y_1 = x_1\mu + \kappa$ y $y_2 = x_2\mu + \kappa$ para algunos $\mu, \kappa \in \mathcal{Q}$ y como $x_1 = x_2$, entonces $y_1 = y_2$.

Si $x_1 \neq x_2$, vemos que para que se satisfagan simultáneamente $y_1 = x_1\mu + \kappa$ y $y_2 = x_2\mu + \kappa$ debe ocurrir que

$$y_1 - y_2 = x_1\mu - x_2\mu = (x_1 - x_2)\mu.$$

Entonces

$$\mu = (x_1 - x_2)^{-1}(y_1 - y_2).$$

Obtenemos κ de la siguiente manera: $\kappa = y_1 - x_1\mu = y_1 - x_1(x_1 - x_2)^{-1}(y_1 - y_2)$. Además obtenemos el mismo valor para κ de la ecuación $\kappa = y_2 - x_2\mu$. Así A y B satisfacen la ecuación $y = x(x_1 - x_2)^{-1}(y_1 - y_2) - (y_1 + x_1(x_1 - x_2)^{-1}(y_1 - y_2))$.

La recta es única porque las ecuaciones determinan de manera única a μ y κ y claramente no hay recta $x = \lambda$ que pase por los dos puntos. De aquí se concluye el primer inciso.

Sea l una recta y P un punto que no está en l . Si l es una recta de tipo $y = x\mu + k$ entonces la recta $y = x\mu + (b - a\mu)$ pasa por $P = (a, b)$ y no intersecta a l . Por otro

lado, cualesquiera rectas $y = x\mu_1 + k_1$ y $y = x\mu_2 + k_2$ tienen un punto en común si $\mu_1 \neq \mu_2$, ya que por el teorema 3.14 existe una única solución para el sistema de ecuaciones. Además, cualquier recta $x = \lambda$ intersecciona a una recta $y = x\mu + \kappa$ en el punto $(\lambda, \lambda\mu + \kappa)$. Por lo tanto la recta construida es única.

Sea l una recta de tipo $x = \lambda$ y (a, b) un punto que no está en l , entonces $\lambda \neq a$. Así que la recta $x = a$ no intersecciona a l y pasa por (a, b) . Por otro lado cualquier recta $y = x\mu + \kappa$ intersecciona a $x = \lambda$ en $(\lambda, \lambda\mu + \kappa)$. Esto prueba el segundo inciso.

■

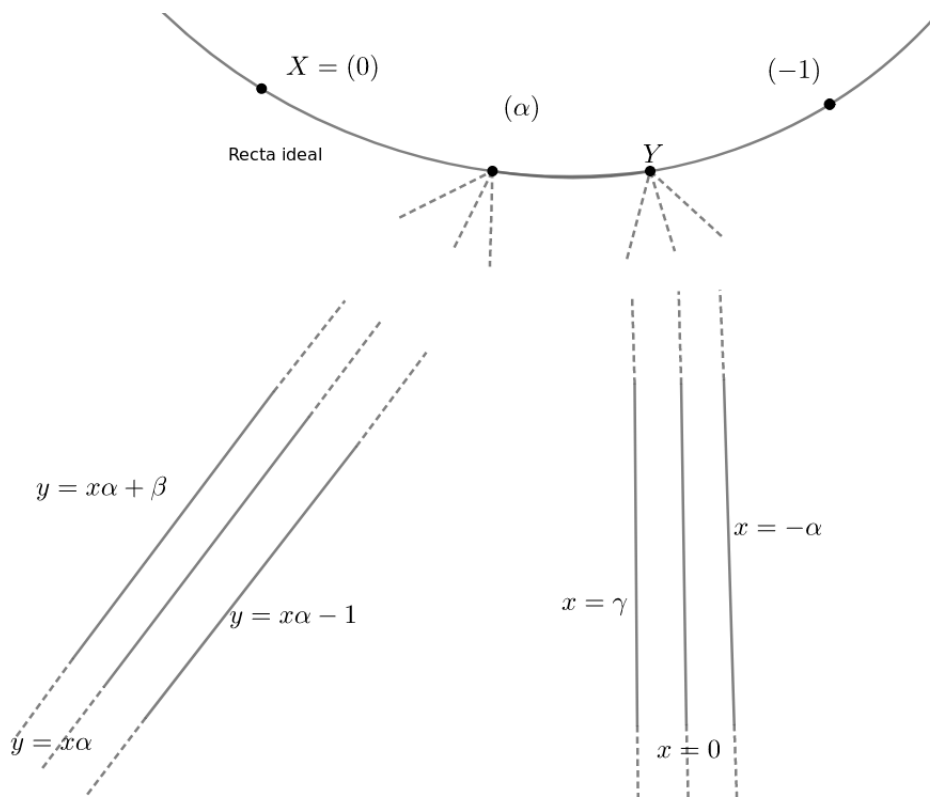
El teorema anterior establece que para cada $\mu \in \mathcal{Q}$ existe una familia de rectas $\{y = x\mu + \kappa : \kappa \in \mathcal{Q}\}$ tales que éstas no se interseccionan dos a dos. Para cada $\mu \in \mathcal{Q}$ agregamos un punto (μ) al conjunto Ω' , y lo añadimos a las 9 rectas de la forma $y = x\mu + \kappa$. Entonces estas rectas se interseccionan en (μ) . Y a cada una de las rectas $x = \lambda$ agregamos un punto al que llamaremos Y común a todas ellas. Además al punto (0) también lo denotaremos como X . Por último definimos la recta XY que contiene a cada punto de los que acabamos de agregar $XY = \{(\mu) : \mu \in \mathcal{Q}\} \cup \{Y\}$ (ver figura 4.1).

A continuación probaremos que con los puntos y la recta que agregamos conseguimos un conjunto de puntos y rectas que forman un plano proyectivo.

A los puntos del conjunto Ω' los llamamos puntos *propios* y los del conjunto $\{(\mu) : \mu \in \mathcal{Q}\} \cup \{Y\}$ puntos *ideales*. A las rectas $y = x\mu + \kappa$ con $\mu, \kappa \in \mathcal{Q}$ y a las rectas $x = \lambda$ con $\lambda \in \mathcal{Q}$ las llamamos rectas *propias* y la recta XY es llamada recta *ideal*.

Teorema. 4.3. Los puntos $\{(x, y) : x, y \in \mathcal{Q}\}$ junto con los puntos $\{(\mu) : \mu \in \mathcal{Q}\}$ y el punto Y , son los puntos de un plano proyectivo que tiene por rectas a $y = x\mu + \kappa$ con $\mu, \kappa \in \mathcal{Q}$; $x = \lambda$ con $\lambda \in \mathcal{Q}$ y a la recta XY .

Demostración. Veamos primero que entre dos puntos distintos cualesquiera A y B pasa una única recta. Si los dos puntos son propios, tenemos que la recta existe y es única por el teorema 4.2. Si los dos son puntos ideales, la recta ideal pasa por los dos

Figura 4.1: Construcción del plano Ω

y es la única. Supongamos ahora que $A = (x_0, y_0)$ es propio y B es un punto ideal. Cuando $B = Y$, tenemos que las rectas que pasan por Y son la ideal o las de la forma $x = \lambda$, así la única de estas que pasa por A es $x = x_0$. Y si B es igual (μ) , para algún $\mu \in \mathcal{Q}$, la recta $y = x\mu - x_0\mu + y_0$ une a los dos puntos y es la única con esta propiedad.

Ahora probemos que cualesquiera dos rectas se intersectan en un punto. Sean dos rectas l y m distintas. Si l es la recta ideal entonces intersecta a m (una recta propia) en un único punto, el punto ideal de m . Si las dos son rectas propias y tienen la misma pendiente se intersectan en el punto ideal de su clase. Si l es de la forma $y = x\mu + \kappa$ y m de la forma $x = \lambda$ se intersectan en el punto $(\lambda, \lambda\mu + \kappa)$. Resta verificar el caso en que las dos son de la forma $y = x\mu + \kappa$. Sean

$$y = x\mu_1 + \kappa_1,$$

$$y = x\mu_2 + \kappa_2$$

dos rectas distintas. Restando la segunda ecuación a la primera obtenemos

$$0 = x\mu_1 - x\mu_2 + \kappa_1 - \kappa_2,$$

de la cual se sigue que

$$\kappa_2 - \kappa_1 = x\mu_1 - x\mu_2.$$

Como las dos rectas tienen pendientes diferentes alguna pendiente es diferente de 0, digamos μ_1 . Podemos encontrar el valor de x resolviendo la ecuación

$$(\kappa_2 - \kappa_1)\mu_1^{-1} = x - x\mu_2\mu_1^{-1},$$

la cual tiene solución única por el teorema 3.13.

Los puntos $(1, 0)$, $(0, 1)$, $(0, \alpha)$, $(\alpha, 0)$ forman un cuadrángulo regular. Las rectas que pasan por estos 4 puntos son:

$$\begin{aligned} y = -x + 1 & \quad (1, 0), \quad (0, 1), \\ y = 0 & \quad (1, 0), \quad (\alpha, 0), \\ x = 0 & \quad (0, 1), \quad (0, \alpha), \\ y = -x + \alpha & \quad (\alpha, 0), \quad (0, \alpha), \\ y = x(-\alpha) + \alpha & \quad (1, 0), \quad (0, \alpha), \\ y = x\alpha + 1 & \quad (0, 1), \quad (\alpha, 0). \end{aligned}$$

■

Denotaremos al punto $(0, 0)$ como O , ya que lo estaremos utilizando de manera frecuente.

4.2. Plano dual Ω^D

Como vimos el dual de un plano proyectivo es un plano proyectivo. El dual de Ω tiene por puntos a las rectas de Ω , es decir, las rectas $[\mu, \kappa]$, $[\lambda]$ y a la recta ideal. Además tiene por rectas a los puntos (lápices de rectas) de Ω que son las parejas (x, y) con $x, y \in \mathcal{Q}$, los puntos (μ) de Ω y Y . Como relaciones de incidencia en Ω tenemos

$$\begin{aligned}
(\rho, \sigma) \in [\mu, \kappa] & \text{ si y sólo si } \sigma = \rho\mu + \kappa, \\
(\rho, \sigma) \in [\lambda] & \text{ si y sólo si } \rho = \lambda, \\
(\rho, \sigma) & \notin XY, \\
(\tau) \in [\mu, \kappa] & \text{ si y sólo si } \tau = \mu, \\
(\tau) & \notin [\lambda], \\
(\tau) & \in XY, \\
Y & \notin [\mu, \kappa], \\
Y & \in [\lambda], \\
Y & \in XY.
\end{aligned}$$

En Ω^D las relaciones de incidencia se obtienen revirtiendo las incidencias en Ω . Para cada resultado en el plano Ω tenemos un resultado dual en Ω^D . Con esto probaremos en la sección 4.4 que Ω no es isomorfo a su propio dual.

4.3. Colineaciones en Ω

Las colineaciones de Ω nos ayudaran a ver que el plano no es desarguesiano ni isomorfo a su dual. Las operaciones de suma y multiplicación en los minicuaternios determinan colineaciones que veremos en las secciones 4.3.1 y 4.3.2.

A los 10 puntos de la recta XY los dividimos en los siguientes 5 bloques, a los cuales vamos a llamar *parejas imprimitivas*:

$$\{X = (0), Y\}; \{(1), (-1)\}; \{(\alpha), (-\alpha)\}; \{(\beta), (-\beta)\}; \{(\gamma), (-\gamma)\}. \quad (4.1)$$

4.3.1. Colineación $\tau_{\varepsilon, \delta}$

Dados $\varepsilon, \delta \in \mathcal{Q}$ definimos las siguientes funciones en Ω .

$$\tau_{\varepsilon, \delta} : (x, y) \mapsto (x + \varepsilon, y + \delta).$$

Veamos que se extienden a colineaciones de Ω .

Bajo una colineación, cualquier recta debe ir a otra recta. Consideremos primero las rectas $y = x\mu + \kappa$ y recordemos que cualquier punto (x_0, y_0) en una de ellas es tal que $y_0 = x_0\mu + \kappa$. Notemos que

$$y_0 + \delta = x_0\mu + \kappa + \delta = (x_0 + \varepsilon)\mu + \kappa + \delta - \varepsilon\mu,$$

de donde se sigue que $\tau_{\varepsilon, \delta}(x_0, y_0)$ está en la recta

$$y = x\mu + \kappa + \delta + \varepsilon\mu$$

para cualquier punto (x_0, y_0) en la recta $y = x\mu + \kappa$.

Si la recta es $x = \lambda$, sus puntos son de la forma (λ, y_0) , de donde $\tau_{\varepsilon, \delta}(\lambda, y_0) = (\lambda + \varepsilon, y_0 + \delta)$ y está en la recta $x = \lambda + \varepsilon$.

Visto lo anterior definimos $\tau_{\varepsilon, \delta}(\mu) = \mu + \varepsilon$ y $\tau_{\varepsilon, \delta}(Y) = Y$. Bajo $\tau_{\varepsilon, \delta}$, la recta XY va a ella misma, $y = x\mu + \kappa$ va a la recta $y = x\mu + \kappa + \delta + \varepsilon\mu$ y la recta $x = \lambda$ va a la recta $x = \lambda + \varepsilon$.

Cada colineación $\tau_{\varepsilon, \delta}$ fija a cada punto de XY , entonces es una colineación axial, y por la proposición 1.18 es una colineación central. Podemos ver que $\tau_{\varepsilon, \delta}$ es una elación con la recta ideal como eje; cuando $\varepsilon \neq 0$ tiene centro $(\varepsilon^{-1}\delta)$ y cuando $\varepsilon = 0$ el centro es Y . Probaremos esto en la siguiente proposición.

Proposición. 4.4. $\tau_{\varepsilon, \delta}$ es una elación que tiene por eje a la recta ideal; cuando $\varepsilon \neq 0$ tiene centro $(\varepsilon^{-1}\delta)$ y cuando $\varepsilon = 0$ su centro es Y .

Demostración. Como vimos la recta XY está fija punto por punto bajo $\tau_{\varepsilon, \delta}$. Supongamos que $\varepsilon \neq 0$ y tomemos un punto $P = (x_0, y_0)$. La recta que pasa por P y $(\varepsilon^{-1}\delta)$ es $y = x(\varepsilon^{-1}\delta) - x_0(\varepsilon^{-1}\delta) + y_0$; la imagen de P bajo $\tau_{\varepsilon, \delta}$ también está en esa recta, por lo tanto las rectas que pasan por $(\varepsilon^{-1}\delta)$ son invariantes y así éste es el centro.

Si $\varepsilon = 0$ entonces $\tau_{\varepsilon, \delta}$ manda a P en $(x_0, y_0 + \delta)$, la recta YP es $x = x_0$. Entonces permuta los puntos de esta recta. Se sigue de aquí que las rectas que pasan por Y son invariantes y por lo tanto Y es el centro.

■

4.3.2. Colineación $\zeta_{\rho,\sigma}$

Para $\rho, \sigma \in \mathcal{Q} \setminus \{0\}$ definimos la función $\zeta_{\rho,\sigma}$ en Ω como

$$\zeta_{\rho,\sigma} : (x, y) \mapsto (x\rho, y\sigma).$$

Ahora veamos que $\zeta_{\rho,\sigma}$ puede extenderse a una colineación de Ω . Tomemos una recta cualquiera l . Si l es de la forma $y = x\mu + \kappa$ entonces dado cualquier punto (x_0, y_0) en esa recta tenemos que se satisface que:

$$y_0 = x_0\mu + \kappa,$$

de donde vemos que

$$y_0\sigma = (x_0\mu + \kappa)\sigma = x_0\mu\sigma + \kappa\sigma = (x_0\rho)(\rho^{-1}\mu\sigma) + \kappa\sigma.$$

Esto implica que cada una de la imágenes de los puntos de la recta están en la recta $y = x(\rho^{-1}\mu\sigma) + \kappa\sigma$.

En caso de que la recta sea de la forma $x = \lambda$, la imagen bajo $\zeta_{\rho,\sigma}$ del punto (λ, y_0) es $(\lambda\rho, y_0\sigma)$ y estará en la recta $x = \lambda\rho$, con lo que vemos que $\zeta_{\rho,\sigma}$ fija al punto Y . La recta XY va a sí misma porque el punto (μ) va al punto $(\rho^{-1}\mu\sigma)$ y Y va a Y .

Proposición. 4.5. $\zeta_{\rho,1}$ es una (X, OY) -homología.

Demostración. Como vimos anteriormente, (μ) bajo la colineación $\zeta_{\rho,1}$ va a $(\rho^{-1}\mu)$, entonces $X = (0)$ queda fijo. Recordemos que la recta OY es la recta $x = 0$, y cada punto en esta recta queda fijo bajo la colineación $\zeta_{\rho,1}$. De aquí concluimos que la recta OY queda fija punto por punto. Por último, si tomamos un punto $P = (x_0, y_0)$ con $x_0 \neq 0$, entonces la recta que pasa por P y X es $y = y_0$; notemos que $\zeta_{\rho,1}(x_0, y_0) = (x_0\rho, y_0)$ y este punto también pertenece a la recta XP . Por lo tanto X es el centro y OY el eje. ■

De manera análoga se prueba que $\zeta_{1,\rho}$ es una (Y, OX) -homología. En general las colineaciones $\zeta_{\rho,\sigma}$ no son colineaciones centrales.

4.3.3. Colineaciones \mathcal{R} y \mathcal{U}

Ahora estudiemos a la función $\mathcal{R} : (x, y) \mapsto (y, x)$. Es inmediato que es una función biyectiva en el conjunto de puntos propios. Si (x_0, y_0) está en la recta $y = x\mu + \kappa$ con $\mu \neq 0$ entonces $y_0 = x_0\mu + \kappa$, de donde se sigue que $y_0\mu^{-1} = x_0\mu\mu^{-1} + \kappa\mu^{-1}$. Despejando x_0 obtenemos $x_0 = y_0\mu^{-1} - \kappa\mu^{-1}$, de modo que $\mathcal{R}(x_0, y_0)$ está en la recta $y = x\mu^{-1} - \kappa\mu^{-1}$. Ahora, las imágenes de las rectas $x = \lambda$ son las rectas $y = \lambda$, y viceversa. Por lo que \mathcal{R} se extiende un colineación de Ω que manda (μ) a (μ^{-1}) con $\mu \neq 0$ e intercambia X y Y .

La función $\mathcal{U} : (x, y) \mapsto (x + y, y - x)$ es una función biyectiva, ya que tiene por inversa a la función \mathcal{U}' que envía $(x, y) \mapsto (y - x, -x - y)$. Verifiquemos que \mathcal{U} y \mathcal{U}' son funciones inversas:

$$\mathcal{U}'\mathcal{U}(x, y) = \mathcal{U}'(x + y, y - x) = ((y - x) - (x + y), -(x + y) - (y - x)) = (x, y).$$

Además es una función que manda puntos propios colineales en puntos propios colineales. Tomemos una recta de la forma $y = x\mu + \kappa$ con $\mu \in \mathcal{Q}^*$. Un punto (x_0, y_0) en ella será tal que $y_0 = x_0\mu + \kappa$. Así

$$\begin{aligned} x_0 - y_0 &= x_0 - x_0\mu - \kappa \\ &= (x_0 - x_0\mu)\mu\mu^{-1} - \kappa \\ &= (x_0\mu - x_0\mu^2)\mu^{-1} - \kappa. \end{aligned} \tag{4.2}$$

Ya que $\mu^2 = -1$ tenemos que

$$\begin{aligned} x_0 - y_0 &= (x_0\mu + x_0)\mu^{-1} - \kappa \\ &= (y_0 - \kappa + x_0)\mu^{-1} - \kappa \\ &= (y_0 + x_0)\mu^{-1} - \kappa\mu^{-1} - \kappa \\ &= (y_0 + x_0)(-\mu) + \kappa\mu - \kappa. \end{aligned} \tag{4.3}$$

Con lo cual vemos que si $\mu \in \mathcal{Q}^*$, la imagen de la recta $y = x\mu + \kappa$ bajo \mathcal{U} es la recta $y = x(-\mu) + \kappa\mu - \kappa$.

Consideremos una recta que tiene por ecuación $y = x + \kappa$. Un punto (x_0, y_0) en la recta satisface que $y_0 = x_0 + \kappa$. Esto implica que $y_0 - x_0 = \kappa$ y la imagen del punto estará en la recta $y = -\kappa$. Por otro lado, si (x_0, y_0) es un punto de la recta $y = -x + \kappa$ tenemos que $y_0 + x_0 = \kappa$ y la recta va a la recta $x = \kappa$. Por último, si (x_0, y_0) es un punto de la recta $y = \kappa$ entonces $y_0 = \kappa$. Así que

$$\begin{aligned} x_0 - y_0 &= x_0 + y_0 + y_0 \\ &= x_0 + y_0 + \kappa. \end{aligned} \tag{4.4}$$

Por lo tanto la recta $y = \kappa$ bajo la función \mathcal{U} va a la recta $y = x - \kappa$.

Sólo resta considerar las rectas de la forma $x = \lambda$. Un punto (x_0, y_0) en la recta $x = \lambda$ satisface que $x_0 = \lambda$ y entonces

$$\begin{aligned} x_0 - y_0 &= x_0 - y_0 + x_0 - x_0 \\ &= x_0 + x_0 - y_0 - x_0 \\ &= -x_0 - y_0 - x_0 \\ &= x_0(-1) + y_0(-1) - \lambda \\ &= (x_0 + y_0)(-1) - \lambda \end{aligned} \tag{4.5}$$

por lo que la recta $x = \lambda$ tiene por imagen a la recta $y = x(-1) - \lambda$.

Para extender a \mathcal{U} definimos $\mathcal{U}((0)) := (1)$, $\mathcal{U}((Y)) := (-1)$, $\mathcal{U}((1)) := (0)$, $\mathcal{U}((-1)) := Y$ y $\mathcal{U}(\mu) := (-\mu)$ con $\mu \neq 1, -1, 0$.

4.3.4. Colineaciones dadas por automorfismos

En el capítulo 2 hablamos de los automorfismos del casi-campo de los mini-cuaternos. Dado un automorfismo \mathcal{F} que envía a α en el elemento σ definimos $\mathcal{A}_\sigma : (x, y) \mapsto (\mathcal{F}(x), \mathcal{F}(y))$.

Veamos que podemos extender \mathcal{A}_σ a una colineación de Ω . Primero probaremos que los puntos propios colineales van a puntos propios colineales y luego definiremos la función en los puntos ideales. Sea una recta de tipo $x = \lambda$ un punto en ella es de la forma (λ, y_0) . Bajo la función \mathcal{A}_σ su imagen es $(\mathcal{A}_\sigma(\lambda), \mathcal{A}_\sigma(y_0))$ que es un punto en la recta $x = \mathcal{A}_\sigma(\lambda)$, por lo que los puntos propios de $x = \lambda$ van a los puntos propios

de la recta $x = \mathcal{A}_\sigma(\lambda)$. En una recta con ecuación $y = x\mu + \kappa$ un punto (x_0, y_0) que pertenece a ella satisface que $y_0 = x_0\mu + \kappa$, y como \mathcal{F} es un automorfismo se satisface que $\mathcal{F}(y) = \mathcal{F}(x)\mathcal{F}(\mu) + \mathcal{F}(\kappa)$. Con lo cual vemos que $\mathcal{A}_\sigma((x_0, y_0)) = (\mathcal{F}(x_0), \mathcal{F}(y_0))$ pertenece a la recta $y = x\mathcal{F}(\mu) + \mathcal{F}(\kappa)$. En los puntos de la recta XY definimos \mathcal{A}_σ como $\mathcal{A}_\sigma((\mu)) := (\mathcal{F}(\mu))$, en particular la imagen del punto $X = (0)$ es X . Definimos $\mathcal{A}(Y) := Y$.

4.4. Transitividad en Ω

En esta sección analizamos si dado un punto P y una recta l existe o no una (P, l) -colineación distinta de la identidad, y más aún, si Ω es (P, l) -transitivo. Esto nos ayudará a concluir que el plano no es desarguesiano (teorema 1.21).

Anteriormente vimos que las siguientes son colineaciones.

$$\begin{aligned} \tau_{\varepsilon, \delta} : (x, y) &\mapsto (x + \varepsilon, y + \delta), \\ (\mu) &\mapsto (\mu), \\ Y &\mapsto Y. \end{aligned} \tag{4.6}$$

$$\begin{aligned} \zeta_{\rho, \sigma} : (x, y) &\mapsto (x\rho, y\sigma), \\ (\mu) &\mapsto (\rho^{-1}\mu\sigma), \\ Y &\mapsto Y(\rho, \sigma \neq 0). \end{aligned} \tag{4.7}$$

$$\begin{aligned} \mathcal{R} : (x, y) &\mapsto (y, x), \\ X &\mapsto Y, Y \mapsto X, \\ (\mu) &\mapsto (\mu^{-1}) \text{ para } \mu \neq 0. \end{aligned} \tag{4.8}$$

$$\begin{aligned} \mathcal{U} : (x, y) &\mapsto (x + y, x - y), \\ (0) &\mapsto (1), (1) \mapsto (0), \\ (-1) &\mapsto Y, Y \mapsto (-1), \\ (\mu) &\mapsto (-\mu) \text{ con } \mu \neq 0, 1, -1. \end{aligned} \tag{4.9}$$

$$\begin{aligned} \mathcal{A}_\lambda : (x, y) &\mapsto (\mathcal{F}(x), \mathcal{F}(y)) \\ (\mu) &\mapsto (\mathcal{F}(\mu)), Y \mapsto Y. \end{aligned} \tag{4.10}$$

donde \mathcal{F} es un automorfismo tal que $\mathcal{F}(\alpha) = \lambda \in \mathcal{Q}^*$

Proposición. 4.6. Las funciones descritas en (4.6), (4.7), (4.8), (4.9) y (4.10) son colineaciones de Ω . Además permutan a las parejas imprimitivas descritas en (4.1).

Demostración. En la sección 4.3 vimos que todas estas funciones son colineaciones, además de que

- $\tau_{\varepsilon, \delta}$ deja a cada punto ideal fijo.
- $\zeta_{\rho, \sigma}$ deja fija a la pareja $\{X, Y\}$ pues deja fijo a cada uno de ellos. Por otro lado, manda a la pareja $\{(\mu), (-\mu)\}$ en $(\rho^{-1}\mu\sigma), (-\rho^{-1}\mu\sigma)$.
- Cuando aplicamos \mathcal{R} , el punto (μ) va a (μ^{-1}) para $\mu \neq 0$. X y Y se intercambian.
- En la colineación \mathcal{U} tenemos que $\mathcal{U}(0) = (1)$, $\mathcal{U}(Y) = (-1)$, $\mathcal{U}(1) = (0)$, $\mathcal{U}(-1) = Y$ y $\mathcal{U}(\mu) = (-\mu)$ si $\mu \neq 0, 1, -1$.
- Dada una colineación \mathcal{A}_λ y $\mu \neq 0$, como \mathcal{F} es un automorfismo entonces $\mathcal{F}(-\mu) = -\mathcal{F}(\mu)$. Por otro lado X, Y son puntos fijos.

■

La proposición 4.3 prueba que las parejas imprimitivas conforman un sistema de bloques de imprimitividad [10] bajo el grupo de colineaciones generado por las colineaciones $\tau_{\varepsilon, \delta}, \zeta_{\rho, \sigma}, \mathcal{R}, \mathcal{U}, \mathcal{A}_\lambda$.

Con los siguientes lemas veremos que existen colineaciones que permutan las parejas imprimitivas de manera transitiva, es decir, dadas dos parejas existe una colineación que manda la primera en la segunda.

Lema. 4.7. Si $\mu \neq 0$ hay una colineación que manda (μ) a X y $(-\mu)$ a Y .

Demostración. Recordemos primero que $\mathcal{U}(X) = 1$, $\mathcal{U}(Y) = -1$ y $\zeta_{\mu, 1}(\mu) = (\mu^{-1} \times \mu \times 1) = (1)$. Como la colineación permuta las parejas imprimitivas se satisface que $\zeta_{\mu, 1}(-\mu) = (-1)$. De lo anterior tenemos que $(\mathcal{U}^{-1} \circ \zeta_{\mu, 1})(\mu) = (X)$ y $(\mathcal{U}^{-1} \circ \zeta_{\mu, 1})(-\mu) = (Y)$.

■

Lema. 4.8. Dadas dos parejas imprimitivas $\{V_1, W_1\}$ y $\{V_2, W_2\}$ existe una colineación que manda V_1 a V_2 y W_1 a W_2 .

Demostración. Por el lema anterior existen colineaciones \mathcal{F}_i que mandan V_i a X y W_i a Y , para $i = 1, 2$. Entonces $\mathcal{F}_2^{-1}\mathcal{F}_1$ es la colineación buscada. ■

Tenemos un resultado similar al lema 4.8. Para cualesquiera dos puntos propios existe una colineación que los envía a otros dos puntos propios. Este resultado está expuesto en el siguiente lema.

Lema. 4.9. Dados dos puntos propios distintos A y B , y dos puntos propios distintos A' y B' , existe una colineación que manda A en A' y B en B' .

Demostración. Primero probemos que dados cualesquiera dos A y B existe una colineación que manda A a $(0, 0)$, y B a $(1, 0)$. Tomemos las rectas AB y XY . Hay una colineación que manda el punto $Z = AB \cap XY$ a X . Si $Z = (\mu)$ existe por el lema 4.8. Si $Z = Y$, tenemos que $\mathcal{R}(Y) = X$. Supongamos que mediante esta colineación A va a $A_1 = (\rho, \sigma)$ y B a cierto punto B_1 . La colineación $\tau_{-\rho, -\sigma}$ manda A_1 a $(0, 0)$, a B_1 a cierto punto B_2 y deja a X fijo. Como A, B, Z son colineales sus imágenes van a la misma recta bajo la composición de las colineaciones anteriores, así X , $(0, 0)$ y B_2 , están en la recta $y = 0$, por lo que $B_2 = (\tau, 0)$. Con $\zeta_{\tau-1, 1}$ B_2 va a $(1, 0)$ mientras que X y $(0, 0)$ se quedan fijos. De manera análoga encontramos una colineación que mande A' y B' a $(0, 0)$ y a $(1, 0)$. ■

Observación. 4.10. De la proposición anterior, concluimos que dadas dos rectas propias existe una colineación que envía una en la otra.

En los siguientes resultados mostramos parejas (P, l) con P un punto y l una recta para las que Ω resulta ser (P, l) -transitivo.

Teorema. 4.11. Ω es (W, XY) -transitivo para toda $W \in XY$.

Demostración. Si $W = Y$, por la proposición 4.4 sabemos que $\tau_{0, \varepsilon}$ es una elación con centro Y y eje XY ; como hay una para cada $\varepsilon \in \mathcal{Q}$ tenemos que hay 9 elaciones diferentes. De igual forma si $W = (\mu)$, tenemos que $\tau_{\varepsilon, \varepsilon\mu}$ es una (W, XY) -elación por la proposición 4.4 con lo cual obtenemos 9 $((\mu), XY)$ -elaciones diferentes, una para cada $\varepsilon \in \mathcal{Q}$. Por el teorema 1.20 concluimos que Ω es (W, XY) -transitivo. ■

Teorema. 4.12. Ω es (X, OY) -transitivo y (Y, OX) transitivo.

Demostración. Para cada $\rho \in \mathcal{Q} \setminus \{0\}$ tenemos que $\zeta_{\rho,1}$ es una (X, OY) -homología por la proposición 4.5, entonces tenemos 8 homología distintas y por el teorema 1.20, Ω es (X, OY) -transitivo. De manera análoga Ω es (Y, OX) transitivo ya que $\zeta_{1,\rho}$ es una (Y, OX) -homología. ■

Recordemos que dado un punto propio $P = (\varepsilon, \delta)$ la colineación $\tau_{\varepsilon,\delta}$ fija a X y a Y , además envía O a P . Por lo que tenemos el siguiente corolario que se sigue del teorema 1.19.

Corolario. 4.13. Si P es un punto propio tenemos que

- i) Ω es (X, PY) -transitivo y (Y, PX) -transitivo.
- ii) Ω es (W, PW') -transitivo, para W, W' una pareja imprimitiva.

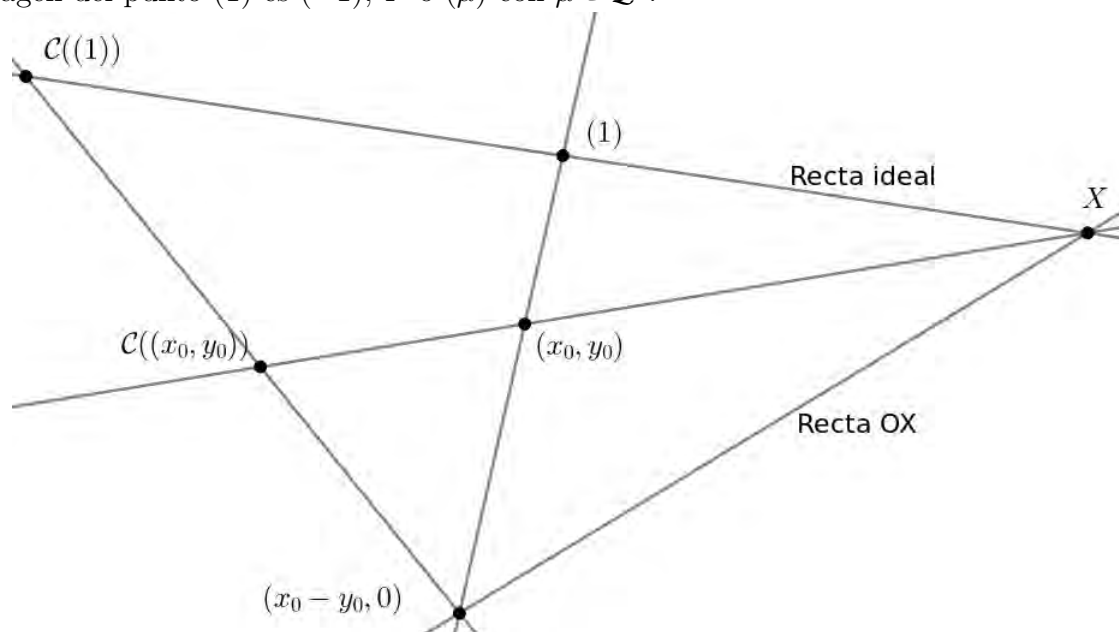
Demostración. Sea $P = (x_0, y_0)$. Tenemos que Ω es (X, OY) -transitivo por el teorema 4.12. Como τ_{x_0,y_0} es una colineación, Ω es $(\tau_{x_0,y_0}(X), \tau_{x_0,y_0}(O)\tau_{x_0,y_0}(Y))$ -transitivo por el teorema 1.19. Además X y Y son puntos fijos bajo τ_{x_0,y_0} , mientras que $\tau_{x_0,y_0}(O) = P$. De manera análoga probamos el plano es (Y, PX) -transitivo lo que concluye la prueba del primer inciso.

De manera análoga, usando el teorema 4.12 vemos que Ω es (W, PW') -transitivo ya que la pareja imprimitiva $\{X, Y\}$ puede enviarse mediante una colineación a cualquier otra pareja imprimitiva (ver teorema 1.19 y lema 4.8). ■

No para cualquier punto P y recta l existe una (P, l) -colineación diferente de la identidad. Por ejemplo no existen colineaciones no triviales con centro X y eje OX .

Para verificar los anterior supongamos que hay una (X, OX) -colineación \mathcal{C} . Como X es el centro, tenemos que bajo \mathcal{C} los puntos de una recta que pasa por X se permutan entre ellos. La recta que pasa por un punto (x_0, y_0) y X es la recta $y = y_0$, así que la imagen de (x_0, y_0) es un punto (x'_0, y_0) con $x'_0 \in \mathcal{Q}$. De la misma manera la imagen de un punto ideal diferente de X es un punto en la recta ideal ya que la recta XY es invariante.

Analicemos las posibles imágenes del punto (1). La imagen de (1) no puede ser X , ya que X es un punto fijo bajo una (X, OX) -colineación y la única colineación que envía (1) a (1) es la colineación identidad. Falta analizar los casos donde la imagen del punto (1) es (-1) , Y o (μ) con $\mu \in \mathcal{Q}^*$.



Lema. 4.14. No existe una (X, OX) -colineación en la que la imagen de (1) es Y .

Demostración. Los puntos (1) , (x_0, y_0) y $(x_0 - y_0, 0)$ pertenecen a la recta $y = x - x_0 + y_0$. Así que los puntos $\mathcal{C}((1)) = Y$, $\mathcal{C}((x_0 - y_0, 0)) = (x_0 - y_0, 0)$ y $\mathcal{C}(x_0, y_0) = (x'_0, y_0)$ también son colineales. Como Y y $(x_0 - y_0, 0)$ están en la recta $x = x_0 - y_0$ se deduce que $x'_0 = x_0 - y_0$. Por lo tanto la imagen de un punto (x_0, y_0) es $(x_0 - y_0, y_0)$.

Por otro lado los puntos $(0, 0)$, $(1, \alpha)$ y $(\alpha, -1)$ están en la recta $y = x\alpha$. Sin embargo los puntos $\mathcal{C}(0, 0) = (0, 0)$, $\mathcal{C}(1, \alpha) = (-\beta, \alpha)$ están en la recta $y = x(-\gamma)$, mientras que $\mathcal{C}(\alpha, -1) = (\gamma, -1)$ no pertenece a esa recta. ■

Lema. 4.15. No existe una (X, OX) -colineación en la que la imagen de (1) es (-1) .

Demostración. Sea \mathcal{C} es una (X, OX) -colineación tal que $\mathcal{C}((1)) = (-1)$. De manera análoga al lema 4.14 vemos que (-1) , (x'_0, y_0) y $(x_0 - y_0, 0)$ son puntos colineales que pertenecen a la recta $y = x(-1) + x_0 - y_0$ y obtenemos que $x'_0 = x_0 + y_0$.

Como en el caso anterior, los puntos colineales $(0, 0)$, $(1, \alpha)$ y $(\alpha, -1)$ no van a puntos colineales, ya que $\mathcal{C}(0, 0) = (0, 0)$, $\mathcal{C}(1, \alpha) = (\gamma, \alpha)$ y $\mathcal{C}(\alpha, -1) = (\beta, -1)$; el

primero y el último están en la recta $y = x\beta$, pero el punto (γ, α) no pertenece a dicha recta. ■

Por último consideremos el caso en que la imagen de (1) es un punto (μ) con $\mu \in \mathcal{Q}^*$.

Lema. 4.16. No existe una (X, OX) -colineación en la que la imagen de (1) es (μ) con $\mu \in \mathcal{Q}^*$.

Demostración. Las colineaciones \mathcal{A}_σ de la proposición 4.6 fijan a X y a la recta OX . Para cada punto (μ) , hay una colineación \mathcal{A}_μ que envía el punto (α) a (μ) , por lo que basta verificar que no existen (X, OX) -colineaciones no triviales en la que la imagen de (1) sea (α) . Supongamos que el punto (α) es la imagen del punto (1) bajo la (X, OX) -colineación \mathcal{F} . Consideremos los puntos (α) , $(x_0 - y_0, 0)$ y (x'_0, y_0) que son colineales y pertenecen a la recta $y = x\alpha + y_0\alpha - x_0\alpha$ de donde vemos que $x'_0 = y_0\alpha^{-1} + x_0 - y_0$.

Es fácil ver que los puntos $(0, 0)$, $(1, -1)$ y $(-\alpha, \alpha)$ pertenecen a la recta $y = -x$. Pero $\mathcal{C}(0, 0) = (0, 0)$,

$$\mathcal{C}(1, -1) = (\alpha + 1 + 1, -1) = (\alpha - 1, -1) = (\beta, -1),$$

$$\mathcal{C}(-\alpha, \alpha) = (\alpha\alpha^{-1} - \alpha - \alpha, \alpha) = (1 + \alpha, \alpha) = (\gamma, \alpha),$$

no son colineales, ya que los puntos $(0, 0)$ $(\beta, -1)$ están en la recta $y = x\beta$ y el punto (γ, α) no está contenido en dicha recta. ■

Corolario. 4.17. Si l es una recta propia y L es el punto ideal que está en l , no hay una (L, l) -elación además de la trivial.

Demostración. Si existiera una (L, l) -elación no trivial, entonces como hay una colineación que manda L a X y l a OX por la observación 4.10, también habría una (X, OX) -elación no trivial contradiciendo el lema 4.16. ■

Observación. 4.18. Como Ω no es (X, OX) transitivo, no es desarguesiano y de esto es claro que no es isomorfo al plano sobre el campo de orden 9.

La recta ideal es una recta esencialmente diferente a las rectas propias, como veremos en el siguiente teorema.

Teorema. 4.19. Cada colineación de Ω manda a la recta ideal en sí misma.

Demostración. Supongamos que hay una colineación \mathcal{C} que manda la recta ideal XY a una recta propia l y sea W el punto ideal en l . Entonces, como Ω es (W, XY) -transitivo con $W \in XY$ por el teorema 4.11, también es $(\mathcal{C}(W), \mathcal{C}(XY))$ -transitivo por el 1.19, lo que contradice el corolario 4.17. ■

Ya vimos que no había colineaciones centrales no triviales que tengan por eje una recta propia y por centro el punto ideal de la recta (corolario 4.17). En el siguiente teorema vemos que no hay colineaciones no triviales con centro un punto propio y eje una recta propia.

Teorema. 4.20. No hay una (P, l) -colineación no trivial, con P un punto propio y l una recta propia.

Demostración. Supongamos que existe dicha colineación, como es no trivial la imagen de la recta ideal es una recta propia m lo cual contradice el teorema 4.19. ■

Teorema. 4.21. Ω no es autodual.

Demostración. Por el teorema 4.11, Ω es (W, XY) -transitivo para todo punto W en XY . Entonces en Ω^D es (XY, w) -transitivo con XY punto de Ω^D y w cualquier recta que pase por él. Por otro lado en Ω , por los teoremas 4.17 y 4.20, tenemos que no hay un punto P para el que el plano sea (P, l) -transitivo para cualquier recta l que pase por P . Por lo tanto el plano Ω no es autodual. ■

Conclusiones

Hay 4 planos proyectivos de orden 9. En esta tesis probamos la existencia de tres de ellos: el plano proyectivo construido sobre el campo de orden 9, el plano Ω (que es diferente del plano del campo por la observación 4.18) y su dual Ω^D . El plano Ω^D no es desarguesiano así que es diferente al plano proyectivo sobre el campo con 9 elementos y por el teorema 4.21 sabemos que es diferente a Ω . El plano Ψ es un cuarto plano de orden 9 que es autodual por lo tanto no es isomorfo a Ω y no es desarguesiano con lo cual vemos que no es isomorfo al del campo. Los detalles de este cuarto plano proyectivo pueden encontrarse en [1].

Bibliografía

- [1] ROOM, T.G; KIRKPATRICK, P.B, *miniquaternion Geometry*, Cambridge University Press, 1971
- [2] HARRIS, JONH; HIRTS, JEFFRY; MONSSINGHOFF, M., *Combinatorics and Graph Theory*, Segunda edición, Springer, 2008.
- [3] OXLEY, JAMES, *Matroid Theory*, Oxford University Press, 1992.
- [4] IONIN, YURI; SHRIKHANDE, MOHAN, *Combinatorics of Symmetric Designs*, Cambriage University Press, 2006.
- [5] ALBERT, A. ADRIAN; SANDLER, REUBEN, *An Introduction to Finite Projective Planes*, New York: Holt, Rinehart and Winston, 1968.
- [6] LENZ, HANFRIED, *Kleiner desarguesscher Satz und Dualitat in projektiven Ebenen*, Segunda edición, Springer, Estados Unidos de América, 1990.
- [7] BARTOLLI, ADRIANO, *Le possibili configurazioni del sistema delle coppie punto-retta (A,a) per cui un piano grafico risulta (A,a) -transitivo*, 1957.
- [8] HARTSHORE, ROBIN, *Foundation of Proyective Geometry*, Harvard University, Estados Unidos de América, 1967.
- [9] TARRY, GASTON, *Le Problème de 36 Officiers* 1901.
- [10] CAMERON, PETER, *Permutation Groups*, Cambriage University Press, 1999.