

# Elementos de matemáticas formalizadas en Isabelle/Isar

Fabián Fernando Serrano Suárez

---

Grupo de Lógica Computacional  
Dpto. de Ciencias de la Computación e Inteligencia Artificial  
Universidad de Sevilla  
Sevilla, 15 de septiembre de 2008



DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN  
E INTELIGENCIA ARTIFICIAL

# Elementos de matemáticas formalizadas en Isabelle/Isar

Memoria presentada por  
Fabián Fernando Serrano Suárez  
como trabajo de investigación  
en el Programa de Doctorado  
*Lógica, Computación e  
Inteligencia Artificial*

Fabián Fernando Serrano Suárez

V. B. Director

José Antonio Alonso Jiménez

Sevilla, 15 de Septiembre de 2008



# Índice

<b>1</b>	<b>Introducción</b>	<b>9</b>
<b>2</b>	<b>Teorema de Cantor</b>	<b>13</b>
2.1	Demostración usual . . . . .	13
2.2	Demostraciones formalizadas del teorema de Cantor . . . . .	14
<b>3</b>	<b>El teorema del punto fijo</b>	<b>19</b>
3.1	Demostración usual . . . . .	19
3.2	Demostración formalizada en Isabelle/Isar . . . . .	20
3.2.1	Formalización del teorema del punto fijo en Isabelle . . . . .	20
3.2.2	Demostraciones del teorema del punto fijo en Isabelle/Isar . . . . .	22
<b>4</b>	<b>El Teorema de Schröder-Bernstein</b>	<b>25</b>
4.1	Introducción . . . . .	25
4.2	Demostración en Isar del Teorema de Schröder-Bernstein . . . . .	27
<b>5</b>	<b>Teoremas básicos de la teoría grupos</b>	<b>39</b>
5.1	Definición clásica de grupo y algunas propiedades . . . . .	39
5.2	Combinando el método de deducción natural y el cálculo ecuacional . . . . .	45
5.3	Demostraciones por inducción . . . . .	46
<b>6</b>	<b>Números primos</b>	<b>51</b>
6.1	Propiedades elementales sobre divisibilidad . . . . .	51
6.2	Teorema principal sobre números primos . . . . .	60

---

<b>7</b>	<b>Números irracionales</b>	<b>63</b>
7.1	Definiciones . . . . .	63
7.2	Lemas sobre números racionales e irracionales . . . . .	64
7.3	Teorema principal . . . . .	65
<b>8</b>	<b>Compleitud de los números reales</b>	<b>67</b>
8.1	Algunos conceptos y lemas sobre números reales . . . . .	68
8.2	Demostración del teorema principal . . . . .	74
<b>9</b>	<b>Geometría proyectiva</b>	<b>77</b>
9.1	Declaración de tipos para la geometría proyectiva . . . . .	77
9.2	Los axiomas de la geometría proyectiva . . . . .	78
9.3	Consecuencias básicas de los axiomas . . . . .	80
9.4	Algunas nociones básicas de la geometría proyectiva . . . . .	104
9.5	Algunas consecuencias de las definiciones . . . . .	106
9.6	Proposición de Desargues . . . . .	109
<b>10</b>	<b>Conclusiones</b>	<b>147</b>







# Capítulo 1

## Introducción

Por formalizar demostraciones matemáticas entendemos, de manera general, el escribir definiciones y pruebas en un lenguaje de ordenador de tal forma que estas puedan ser verificadas formalmente por una máquina. Este estudio mecánico de las matemáticas tiene su inicio con la prueba automática de teoremas; en particular, con los trabajos de Gödel, Skolem, Church, Kleene, Turing, Herbrand y Löwenheim. En 1930 J. Herbrand, en su artículo "Investigations in proof theory", propone un muy importante método mecánico para probar teoremas. A partir de este, se derivaron una serie de procedimientos modernos de prueba de teoremas, que han dado origen a toda una teoría de prueba automática de teoremas.

Actualmente se ha mostrado que la prueba interactiva de teoremas es una técnica apropiada para el desarrollo de teorías formales. Por ejemplo, en la verificación de la demostración, es decir, en la certificación de la validez de una demostración existente de un teorema. Específicamente los demostradores interactivos de teoremas requieren de un usuario humano para orientar al sistema. Dependiendo del grado de automatización, el demostrador puede ser reducido a un verificador de la demostración, en el que el usuario proporciona la demostración de una manera formal, o puede ser usado en tareas importantes de la demostración que se pueden realizar automáticamente. Los sistemas de pruebas automáticas han logrado demostrar una cantidad de teoremas interesantes y difíciles, por ejemplo, el teorema de los cuatro colores. En [15] se hace una descripción de 100 teoremas importantes junto con los respectivos sistemas que han formalizado su demostración.

Entre los sistemas de pruebas automáticas que más han sido utilizados exitosamente por los usuarios, ver [16], están: HOL, Coq, Isabelle, PVS, y Mizar. El aspecto más notable del sistema Mizar, a diferencia de los otros sistemas, es su lenguaje de prueba estructurada, el cual ha sido diseñado para representar de manera formal patrones comunes de pruebas matemáticas. Esta característica ha motivado posteriores investigaciones en el diseño de sistemas de pruebas formales entendibles por las per-

sonas. En este sentido, el ambiente Isabelle/Isar, ver [13] para una descripción detallada del sistema, ha sido implementado con el fin de ser una herramienta para la generación automática de documentos de pruebas formales legibles por las personas, que son compuestos por el usuario y verificados por la máquina.

Isabelle es un asistente de prueba genérico. Isabelle/Isar es una extensión de Isabelle con pruebas estructuradas en el lenguaje Isar ("Intelligible semi-automated reasoning"), similar a las pruebas usuales en matemáticas. Estas pruebas son legibles tanto por las personas como por las máquinas.

El objetivo general de este trabajo es ilustrar cómo se elaboran documentos de pruebas formales y estructuradas en el lenguaje Isar/Hol. Isabelle/Hol es una especialización de Isabelle con lógica de orden superior (HOL), y Isar/Hol es una extensión de Isabelle/Hol. No presentamos una semántica formal de Isar, ver [9], sino que introducimos las características del lenguaje por medio de ejemplos.

El objetivo específico es estudiar la analogía entre la prueba matemática (prueba informal) y la prueba semi-automática en Isar (prueba formal) de algunos resultados de las teorías básicas de las matemáticas.

La metodología utilizada para tal fin fue seleccionar y probar formalmente propiedades en distintas áreas de las matemáticas de forma tal que permitieran mostrar los fundamentos y el uso de las técnicas de composición de pruebas formales del lenguaje Isar. Para la prueba formal de estos resultados se usaron algunas definiciones y teoremas de las diferentes teorías del sistema Isabelle. Otros resultados se demostraron como lemas para la demostración del resultado principal, con el fin de estructurar la correspondiente prueba formal y destacar el uso de conceptos y resultados relevantes en la demostración del teorema central. La descripción de los temas desarrollados es la siguiente.

En el capítulo 1 se presentan varias pruebas formales del teorema de Cantor. Inicialmente se muestra la más aproximada a la prueba usual que aparece en los textos de la teoría de conjuntos y posteriormente utilizando las características de Isar se hacen pruebas menos explícitas, en particular se ilustra el uso de los métodos automáticos para la demostración semi-automática y automática del teorema.

En el capítulo 2 se estudia la prueba formal del teorema del punto fijo de Knaster-Tarski usando la representación en Isabelle de los retículos completos. De igual forma que en la demostración del teorema de Cantor, este ejemplo sintetiza el uso de los elementos de Isar que permiten reproducir en forma mecánica la prueba usual expuesta en los textos de matemáticas. En [13] se describen las componentes del sistema Isabelle/Isar utilizadas para la generación automática del documento que contiene la prueba formal, en analogía a la presentación tradicional que aparece en los textos de matemáticas.

---

En el capítulo 3 se demuestra en Isar el teorema de Schröder-Bernstein como una aplicación particular del teorema del punto fijo en el que el retículo completo es el conjunto potencia de un conjunto. Para la demostración, se siguen las ideas expuestas de la correspondiente demostración en Isabelle que aparece en la librería HOL, /HOL/ex/set.thy.

En el capítulo 4 se formalizan los axiomas de la teoría de grupos y se ilustra el uso del razonamiento ecuacional y del principio de inducción matemática en Isar, para la prueba de propiedades básicas sobre grupos.

En el capítulo 5 se utiliza la formalización de número primo y algunas propiedades sobre divisibilidad para la prueba formal de la siguiente propiedad:  *$p$  y  $p^2 + 2$  son números primos si y solamente si  $p = 3$ .*

En el capítulo 6 se emplea la formalización de los conceptos de número racional e irracional y de la definición de exponenciación en los números reales, para establecer la existencia de una potencia racional en términos de dos números irracionales. La parte central de la prueba se basa en el hecho de que  $\sqrt{2}$  es un número irracional.

En el capítulo 7 se aplica la formalización en Isar de la propiedad de completitud de los números reales para la demostración de algunos resultados sobre funciones de valores reales.

En el capítulo 8 se formalizan los axiomas del plano proyectivo y se verifican mecánicamente algunas de las propiedades de la geometría proyectiva enunciadas en el libro de Heyting [3, cap 2]. En particular, se estudia la prueba formal de la proposición generalizada de Desargues.



# Capítulo 2

## Teorema de Cantor

El teorema de Cantor afirma que la cardinalidad de cualquier conjunto es menor que la cardinalidad de su conjunto potencia; es decir, que no existe una función sobreyectiva de un conjunto en su conjunto potencia. Intuitivamente esto significa que cada conjunto tiene más subconjuntos que elementos. Para su demostración Cantor introdujo la técnica de la diagonalización usada en muchas otras demostraciones de propiedades sobre conjuntos infinitos.

Este teorema puede ser demostrado automáticamente por muchos probadores de teoremas de orden superior, por ejemplo TPS fue el primer sistema que generó una prueba por ordenador, y frecuentemente el teorema es usado como un referente por probadores de teoremas de orden superior, por ejemplo, LEO generó una prueba alternativa. En este capítulo presentamos una demostración usual del teorema de Cantor y distintas formulaciones de la prueba en Isabelle/Isar.

### 2.1 Demostración usual

Una formulación usual del teorema de Cantor es la siguiente:

**Teorema 2.1.1 (Teorema de Cantor)** *Sea  $X$  cualquier conjunto y  $\wp(X)$  su conjunto potencia. Entonces no existe una biyección entre  $X$  y  $\wp(X)$ . Más aún, la cardinalidad de  $\wp(X)$  es estrictamente mayor que la cardinalidad de  $X$ ; es decir,  $|X| < |\wp(X)|$ .*

**Demostración:** La función  $F: X \rightarrow \wp(X)$ , definida por  $F(x) = \{x\}$  para cada  $x \in X$ , es una función inyectiva de  $X$  a  $\wp(X)$ . Esto prueba que  $|X| \leq |\wp(X)|$ . Falta demostrar que  $X$  no es equivalente a  $\wp(X)$ .

Supongamos que existe una función biyectiva  $f: X \rightarrow \wp(X)$ ; nuestro objetivo es mostrar que esta hipótesis conduce a una contradicción.

Consideremos el conjunto  $A \subseteq X$  definido de la siguiente forma:

$$A = \{x \in X \mid x \notin f(x)\}$$

Puesto que  $A \in \wp(X)$  y  $f$  es sobreyectiva, existe un  $a \in X$  tal que  $f(a) = A$ . El elemento  $a$  pertenece o no pertenece al conjunto  $A$ . Si  $a \in A$ , entonces, por la definición de  $A$ , debemos tener que  $a \notin f(a)$ , y puesto que  $f(a) = A$  esto es imposible. Si  $a \notin A$ , entonces, de nuevo por la definición de  $A$ , debemos tener que  $a \in f(A)$ , y esto también es imposible. De esta forma, hemos llegado a una contradicción; por lo tanto,  $|X| < |\wp(X)|$ . □

## 2.2 Demostraciones formalizadas del teorema de Cantor

En la lógica de orden superior, se pueden considerar los tipos como conjuntos. Entonces, el conjunto potencia correspondiente al tipo  $\alpha$  es el conjunto cuyos elementos son del tipo  $\alpha$ ; es decir,  $\alpha$  set.

Con estas consideraciones, la formulación del teorema de Cantor en lógicas de orden superior afirma que para cada función  $f$  de  $\alpha$  en  $\alpha$  set, existe un conjunto en  $\alpha$  que no pertenece al rango de  $f$ . Formalmente,

**theorem Cantor:**

**fixes**  $f :: 'a \Rightarrow 'a$  set

**shows**  $\exists S. S \notin \text{range } f$

La primera demostración que presentamos es una demostración estructurada para obtener una prueba que se aproxime a la demostración usual y que muestre los resultados de la teoría de conjuntos utilizados.

**theorem Cantor-p1:**

**fixes**  $f :: 'a \Rightarrow 'a$  set

**shows**  $\exists A. A \notin \text{range } f$

**proof** (rule exI)

**let**  $?A = \{x. x \notin f x\}$

**show**  $?A \notin \text{range } f$

**proof** (rule notI)

**assume**  $?A \in \text{range } f$

**hence**  $?A \in \{u. \exists x. u = f x\}$  **by** (simp only: full-SetCompr-eq)

**hence**  $\exists x. ?A = f x$  **by** (simp only: mem-Collect-eq)

**then obtain**  $a$  **where**  $?A = f a$  **by** (rule exE)

**show** False

**proof** cases

```

assume  $a \in ?A$ 
hence  $a \notin f a$  by (simp add: mem-Collect-eq)
hence  $a \notin ?A$  using  $(?A = f a)$  by simp
thus False by contradiction
next
assume  $a \notin ?A$ 
hence  $a \in f a$  by (simp add: mem-Collect-eq)
hence  $a \in ?A$  using  $(?A = f a)$  by simp
thus False by contradiction
qed
qed
qed

```

En la demostración anterior del teorema de Cantor se observa lo siguiente:

Se utilizó el método de prueba *rule* con las siguientes reglas de inferencia como argumento

$$\bullet \frac{P x}{\exists x. P x} \quad (\text{exI})$$

$$\bullet \frac{P}{\overline{False}} \quad \frac{\overline{False}}{\neg P} \quad (\text{notI})$$

También se utilizaron los métodos de prueba

$$\bullet \frac{\frac{P}{\overline{Q}} \quad \frac{\neg P}{\overline{Q}}}{Q} \quad (\text{cases})$$

$$\bullet \frac{\neg P \quad P}{R} \quad (\text{contradiction})$$

Los lemas de la teoría de conjuntos que hemos usado son

$$\bullet \{u \mid \exists x. u = f x\} = \text{range } f \quad (\text{full-SetCompr-eq})$$

$$\bullet (a \in \{x \mid P x\}) = P a \quad (\text{mem-Collect-eq})$$

Además, hemos usado la regla de eliminación del cuantificador existencial

$$\bullet \frac{\exists x. P x \quad \bigwedge x. \frac{P x}{Q}}{Q} \quad (exE)$$

El uso de las reglas de inferencia y lemas no es necesario explicitarlo, como se muestra en la siguiente demostración

**theorem** *Cantor-p2:*

**fixes**  $f :: 'a \Rightarrow 'a \text{ set}$

**shows**  $\exists A. A \notin \text{range } f$

**proof**

**let**  $?A = \{x. x \notin f x\}$

**show**  $?A \notin \text{range } f$

**proof**

**assume**  $?A \in \text{range } f$

**hence**  $?A \in \{u. \exists x. u = f x\}$  **by** *auto*

**hence**  $\exists x. ?A = f x$  **by** *simp*

**then obtain**  $a$  **where**  $?A = f a$  **by** *auto*

**show** *False*

**proof** *cases*

**assume**  $a \in ?A$

**hence**  $a \notin f a$  **by** *simp*

**hence**  $a \notin ?A$  **using**  $\langle ?A = f a \rangle$  **by** *simp*

**thus** *False* **by** *contradiction*

**next**

**assume**  $a \notin ?A$

**hence**  $a \in f a$  **by** *simp*

**hence**  $a \in ?A$  **using**  $\langle ?A = f a \rangle$  **by** *simp*

**thus** *False* **by** *contradiction*

**qed**

**qed**

**qed**

También puede eliminarse los detalles de la obtención del elemento del rango como se muestra en la siguiente demostración.

**theorem** *Cantor-p3:*

**fixes**  $f :: 'a \Rightarrow 'a \text{ set}$

**shows**  $\exists A. A \notin \text{range } f$

**proof**

**let**  $?A = \{x. x \notin f x\}$

**show**  $?A \notin \text{range } f$

**proof**

**assume**  $?A \in \text{range } f$



```

then obtain  $a$  where  $?A = f a$  ..
show False
proof cases
  assume  $a \in ?A$ 
  hence  $a \notin f a$  by simp
  hence  $a \notin ?A$  using  $\langle ?A = f a \rangle$  by simp
  thus False by contradiction
next
  assume  $a \notin ?A$ 
  hence  $a \in f a$  by simp
  hence  $a \in ?A$  using  $\langle ?A = f a \rangle$  by simp
  thus False by contradiction
qed
qed
qed

```

Las demostraciones de las contradicciones en cada uno de los casos puede hacerse automáticamente usando el método *blast* como se muestra en la siguiente demostración.

```

theorem Cantor-p4:
  fixes  $f :: 'a \Rightarrow 'a$  set
  shows  $\exists A. A \notin \text{range } f$ 
proof
  let  $?A = \{x. x \notin f x\}$ 
  show  $?A \notin \text{range } f$ 
proof
  assume  $?A \in \text{range } f$ 
  then obtain  $a$  where  $?A = f a$  ..
  show False
proof cases
  assume  $a \in ?A$ 
  show False using  $\langle ?A = f a \rangle$  by blast
next
  assume  $a \notin ?A$ 
  show False using  $\langle ?A = f a \rangle$  by blast
qed
qed
qed

```

Finalmente, mostramos que la prueba puede hacerse de manera automática usando el método *best*.

**theorem** *Cantor-p5*:

**fixes**  $f :: 'a \Rightarrow 'a \text{ set}$

**shows**  $\exists A. A \notin \text{range } f$

**by** *best*

La última demostración establece el teorema automáticamente, pero no podemos determinar de qué forma el sistema ha realizado la prueba ya que no existe un mecanismo para transformar representaciones usadas a nivel interno por Isabelle que nos permita reconstruir la prueba en Isar. Por tanto, la actividad de escribir documentos de pruebas inteligibles en Isar es un proceso creativo.

# Capítulo 3

## El teorema del punto fijo

### 3.1 Demostración usual

En esta capítulo presentamos el enunciado y la demostración del teorema del punto fijo como suele presentarse en los textos de matemáticas.

La formulación más general del teorema del punto fijo de Knaster–Tarski afirma lo siguiente. Sea  $L$  un retículo completo y  $f : L \rightarrow L$  una función monótona. Entonces el conjunto de puntos fijos de  $f$  en  $L$  es también un retículo completo.

Puesto que los retículos no pueden ser vacíos, el teorema en particular garantiza la existencia de por lo menos un punto fijo (aun más del menor punto fijo). Más adelante, esta última afirmación es la que enunciamos y demostramos como el teorema del punto fijo. En muchos casos prácticos, esta es la implicación más importante del teorema. Por ejemplo, en lógica matemática los menores puntos fijos de funciones sobre conjuntos de fórmulas son usados para calcular las semánticas de un programa lógico. En este caso y en muchas aplicaciones más, una versión más especializada del teorema es usada, esto es, considerando a  $L$  como el retículo de todos los subconjuntos de un cierto conjunto ordenado por inclusión.

**Teorema 3.1.1 (Teorema del punto fijo de Knaster-Tarski)** *Sea  $L$  un retículo completo y  $f : L \rightarrow L$  una función monótona. Entonces  $f$  tiene un punto fijo.*

**Demostración:** Sea  $H = \{x \in L \mid f(x) \leq x\}$  y  $a$  el ínfimo de  $H$ . Vamos a demostrar que  $a$  es un punto fijo de  $f$ ; es decir, que  $f(a) = a$ . Para ello, demostraremos que  $f(a) \leq a$  y que  $a \leq f(a)$ .

Para demostrar que  $f(a) \leq a$ , por la definición de  $a$ , basta probar que  $f(a)$  es una cota inferior de  $H$ . En efecto, sea  $x \in H$ . Entonces

- $a \leq x$  (por la definición de  $a$ ),

- $f(a) \leq f(x)$  (porque  $f$  es monótona) y
- $f(x) \leq x$  (porque  $x \in H$ ).

Por tanto,  $f(a)$  es una cota inferior de  $H$ .

Para demostrar que  $a \leq f(a)$ , por la definición de  $a$ , basta probar que  $f(a) \in H$ . En efecto, tenemos que

- $f(a) \leq a$  (por el apartado anterior) y
- $f(f(a)) \leq f(a)$  (por ser  $f$  monótona)

Por lo tanto, usando la definición de  $H$ , tenemos que  $f(a) \in H$ .

□

## 3.2 Demostración formalizada en Isabelle/Isar

### 3.2.1 Formalización del teorema del punto fijo en Isabelle

En primer lugar, vamos a comentar la formalización del teorema en Isabelle/Isar. Para ello, comenzamos exponiendo la representación en Isabelle de los retículos completos a través de la jerarquía de clases.

Un **conjunto ordenado** consta de un conjunto y una relación de orden (es decir, una relación que es reflexiva, antisimétrica y transitiva). En la teoría `Orderings` se define la clase de los tipos ordenados (*order*) en la que se verifican los siguientes axiomas:

- $x \leq x$  (*order-refl*)
- $\llbracket x \leq y; y \leq x \rrbracket \implies x = y$  (*antisym*)
- $\llbracket x \leq y; y \leq z \rrbracket \implies x \leq z$  (*order-trans*)

donde  $\leq$  es la relación de orden.

Un **semirretículo inferior** es un conjunto ordenado tal todo par de elementos del conjunto posee un ínfimo. En la teoría `Lattices` se define la clase de los semirretículos inferiores (*lower-semilattice*) en la que se verifican los siguientes axiomas:

- $\text{inf } x \ y \leq x$  (*inf-le1*)
- $\text{inf } x \ y \leq y$  (*inf-le2*)

- $\llbracket x \leq y; x \leq z \rrbracket \implies x \leq \text{inf } y z$  (*inf-greatest*)

donde  $\text{inf } x y$  es el ínfimo de  $x$  e  $y$ .

Un **semirretículo superior** es un conjunto ordenado tal que todo par de elementos del conjunto posee un supremo. En la teoría `Lattices` se define la clase de los semirretículos superiores (*upper-semilattice*) en la que se verifican los siguientes axiomas:

- $x \leq \text{sup } x y$  (*sup-ge1*)
- $y \leq \text{sup } x y$  (*sup-ge2*)
- $\llbracket y \leq x; z \leq x \rrbracket \implies \text{sup } y z \leq x$  (*sup-least*)

donde  $\text{sup } x y$  es el supremo de  $x$  e  $y$ .

Un **retículo** es un conjunto ordenado  $(S, \sqsubseteq)$  que es semirretículo inferior y semirretículo superior. En la teoría `Lattices` se define la clase de los retículos (*lattice*).

Un **retículo completo** es un retículo en el que todo subconjunto tiene un ínfimo y un supremo. En la teoría `Lattices` se define la clase de los retículos completos (*complete-lattice*) como la clase de los retículos que verifican los siguientes axiomas:

- $x \in A \implies \text{Inf } A \leq x$  (*Inf-lower*)
- $(\bigwedge x. x \in A \implies z \leq x) \implies z \leq \text{Inf } A$  (*Inf-greatest*)
- $x \in A \implies x \leq \text{Sup } A$  (*Sup-upper*)
- $(\bigwedge x. x \in A \implies x \leq z) \implies \text{Sup } A \leq z$  (*Sup-least*)

donde  $\text{Inf } A$  es el ínfimo del conjunto  $A$  y  $\text{sup } A$  es su supremo.

Además del concepto de retículo completo, necesitamos el de función monótona. La definición en Isabelle de función monótona es

- $\text{mono } f = (\forall x y. x \leq y \longrightarrow f x \leq f y)$  (*mono-def*)

Finalmente, el enunciado en Isabelle del teorema del punto fijo es

**theorem**

**fixes**  $f :: 'a::\text{complete-lattice} \Rightarrow 'a$

**assumes**  $\text{mono } f$

**shows**  $\exists a. f a = a$

### 3.2.2 Demostraciones del teorema del punto fijo en Isabelle/Isar

La siguiente prueba del teorema en Isar corresponde de manera muy aproximada a la presentada en la demostración del teorema 3.1.1. El razonamiento utilizado en la demostración original ha sido traducido textualmente en términos de elementos del lenguaje formal de Isar, ver [11].

**theorem**

**fixes**  $f :: 'a::complete-lattice \Rightarrow 'a$

**assumes**  $mono\ f$

**shows**  $\exists a. f\ a = a$

**proof**

**let**  $?H = \{u. f\ u \leq u\}$

**let**  $?a = Inf\ ?H$

**show**  $f\ ?a = ?a$

**proof** (*rule order-antisym*)

**show**  $f\ ?a \leq ?a$

**proof** (*rule Inf-greatest*)

**fix**  $x$

**assume**  $x \in ?H$

**hence**  $?a \leq x$  **by** (*rule Inf-lower*)

**with**  $\langle mono\ f \rangle$  **have**  $f\ ?a \leq f\ x$  **by** (*simp add:mono-def*)

**also from**  $\langle x \in ?H \rangle$  **have**  $\dots \leq x$  **by** (*simp only: mem-Collect-eq*)

**finally show**  $f\ ?a \leq x$ .

**qed**

**show**  $?a \leq f\ ?a$

**proof** (*rule Inf-lower*)

**from**  $\langle mono\ f \rangle$   $\langle f\ ?a \leq ?a \rangle$  **have**  $f\ (f\ ?a) \leq f\ ?a$  **by** (*simp add:mono-def*)

**thus**  $f\ ?a \in ?H$  **by** (*simp only: mem-Collect-eq*)

**qed**

**qed**

**qed**

En la prueba anterior se han indicado explícitamente los lemas utilizados. También puede probarse dejando algunas indicaciones implícitas como se muestra en la siguiente prueba.

**theorem**

**fixes**  $f :: 'a::complete-lattice \Rightarrow 'a$

**assumes**  $mono\ f$

**shows**  $\exists a. f\ a = a$

**proof**

**let**  $?H = \{u. f\ u \leq u\}$

**let**  $?a = Inf\ ?H$

**show**  $f\ ?a = ?a$

```
proof (rule order-antisym)
  show  $f?a \leq ?a$ 
  proof (rule Inf-greatest)
    fix  $x$ 
    assume  $x \in ?H$ 
    hence  $?a \leq x$  by (rule Inf-lower)
    with (mono f) have  $f?a \leq fx$  ..
    also from (x ∈ ?H) have  $\dots \leq x$  ..
    finally show  $f?a \leq x$  .
  qed
  show  $?a \leq f?a$ 
  proof (rule Inf-lower)
    from (mono f) (f?a ≤ ?a) have  $f(f?a) \leq f?a$  ..
    thus  $f?a \in ?H$  ..
  qed
qed
qed
```





# Capítulo 4

## El Teorema de Schröder-Bernstein

### 4.1 Introducción

En este capítulo vamos a presentar la demostración en Isar del famoso teorema de Schröder–Bernstein, a veces conocido como el teorema de Cantor–Bernstein. Cantor demostró el teorema en 1897, pero su demostración usaba un principio equivalente al axioma de elección. Schröder enunció el teorema en 1896. Su demostración, publicada en 1898, tenía algunos problemas y en 1911 publicó una corrección. La primera demostración totalmente satisfactoria la hizo Felix Bernstein y se publicó en 1898 en un libro de Emile Borel. Una demostración más corta fue descubierta por Tarski (1955) como una consecuencia de su teorema del punto fijo. La demostración que formalizaremos en Isar es una adaptación de la de Tarski.

El lenguaje Isar (razonamiento inteligible semi-automático) permite redactar pruebas formales que son verificables automáticamente siguiendo un razonamiento estructurado inteligible para el ser humano. Sin embargo, no siempre resulta fácil construir simultáneamente una prueba estructurada y automatizada; en este caso puede resultar conveniente obtener primero una prueba aplicativa (tactic-style) en Isabelle y con base en esta escribir el texto de la prueba estructurada en Isar. En este capítulo utilizamos esta metodología para escribir en Isar la demostración del teorema de Schröder-Bernstein con base a la prueba del mismo teorema en Isabelle que aparece expuesta en la librería HOL, /HOL/ex/set.thy:

**lemma** *disj-lemma*:  $-(f' X) = g' (-X) \implies f a = g b \implies a \in X \implies b \in X$   
**by** *blast*

**lemma** *surj-if-then-else*:  
 $-(f' X) = g' (-X) \implies \text{surj } (\lambda z. \text{if } z \in X \text{ then } f z \text{ else } g z)$   
**by** (*simp add: surj-def*) *blast*

**lemma** *bij-if-then-else*:

```
inj-on f X  $\implies$  inj-on g (-X)  $\implies$  -(f' X) = g' (-X)  $\implies$ 
  h = ( $\lambda z$ . if z  $\in$  X then f z else g z)  $\implies$  inj h  $\wedge$  surj h
apply (unfold inj-on-def)
apply (simp add: surj-if-then-else)
apply (blast dest: disj-lemma sym)
done
```

**lemma** *decomposition*:  $\exists X. X = - (g' (- (f' X)))$

```
apply (rule exI)
apply (rule lfp-unfold)
apply (rule monoI, blast)
done
```

**theorem** *Schroeder-Bernstein*:

```
inj (f :: 'a => 'b)  $\implies$  inj (g :: 'b => 'a)
 $\implies$   $\exists h$  :: 'a => 'b. inj h  $\wedge$  surj h
apply (rule decomposition [where f=f and g=g, THEN exE])
apply (rule-tac x = ( $\lambda z$ . if z: x then f z else inv g z) in exI)
  — The term above can be synthesized by a sufficiently detailed proof.
apply (rule bij-if-then-else)
apply (rule-tac [4] refl)
apply (rule-tac [2] inj-on-inv)
apply (erule subset-inj-on [OF - subset-UNIV])
apply blast
apply (erule ssubst, subst double-complement, erule inv-image-comp [symmetric])
done
```

Comenzamos explorando las ideas que aparecen en esta prueba reconstruyendo a partir de ella la demostración correspondiente en matemáticas.

El Teorema de Schröder-Bernstein afirma que si  $f : A \rightarrow B$  y  $g : B \rightarrow A$  son dos funciones inyectivas, entonces existe una función biyectiva  $h : A \rightarrow B$ . Para la demostración de este teorema utilizamos el siguiente lema:

**Lema 4.1.1** Sean  $f_1 : X \rightarrow Y$  y  $f_2 : Z \rightarrow W$  funciones biyectivas con  $X \cap Z = \emptyset$  y  $Y \cap W = \emptyset$ , entonces la función  $f_1 \cup f_2 : X \cup Z \rightarrow Y \cup W$  es biyectiva.

Para poder aplicar este lema en la demostración del teorema hay que, en particular, descomponer de manera apropiada los conjuntos  $A, B$  de la forma  $A = X \cup Z$  y  $B = Y \cup W$ , de tal manera que podamos encontrar las funciones  $f_1, f_2$  que satisfagan las hipótesis del lema.

Siguiendo las ideas de la demostración del Teorema de Descomposición de Banach [7, páginas 7–8] obtenemos tal descomposición haciendo  $X$  igual al menor punto fijo de

la función  $F : \wp(A) \rightarrow \wp(A)$  definida por,  $F(W) = A - g[B - f[W]]$  para todo  $W \subseteq A$ . En donde,  $f[W]$  es la imagen de  $W$ , es decir  $f[W] = \{y | \exists x \in W. y = f(x)\}$ .

**Teorema 4.1.2 (El Teorema de Schröder-Bernstein)** Si  $f : A \rightarrow B$  y  $g : B \rightarrow A$  son funciones inyectivas, entonces existe una función biyectiva  $h : A \rightarrow B$ .

**Demostración:** Sea  $X$  el menor punto fijo de la función  $F : \wp(A) \rightarrow \wp(A)$  definida por,  $F(W) = A - g[B - f[W]]$  para todo  $W \subseteq A$ . Entonces,  $A - X = A - F(X) = A - (A - g[B - f[X]]) = g[B - f[X]]$ .

Ahora, consideremos la función  $f_X : X \rightarrow f[X]$  definida por,  $f_X(x) = f(x)$  para todo  $x \in X$ . Entonces  $f_X$  es biyectiva puesto que  $f$  es inyectiva.

De igual forma, definimos la función  $g_{B-f[X]} : B - f[X] \rightarrow g[B - f[X]]$  y puesto que  $g$  es inyectiva,  $g_{B-f[X]}$  es biyectiva, es decir, la función  $g_{B-f[X]} : B - f[X] \rightarrow A - X$  es biyectiva y, por lo tanto la función inversa de  $g_{B-f[X]}$ ,  $(g_{B-f[X]})^{-1} : A - X \rightarrow B - f[X]$  es biyectiva. De lo anterior, por el lema 4.1.1, se concluye que la función  $h : A \rightarrow B$  definida por  $h = f_X \cup (g_{B-f[X]})^{-1}$  es biyectiva. □

El lema 4.1.1 corresponde al lema *surj-if-then-else* de Isabelle y la anterior demostración de la existencia de un punto fijo de la función  $F(W) = A - g(B - f(W))$  corresponde al lema *decomposition*.

## 4.2 Demostración en Isar del Teorema de Schröder-Bernstein

En lo que sigue demostramos en Isar los lemas y el teorema de Schröder-Bernstein enunciados anteriormente en Isabelle, precedido cada uno por su correspondiente demostración en matemáticas.

**Lema 4.2.1 (disj-lemma)** Sean  $f : A \rightarrow B$ ,  $g : A \rightarrow B$ ,  $X \subseteq A$  y  $a, b \in A$  tales que,  $B - f[X] = g[A - X]$ ,  $f(a) = g(b)$  y  $a \in X$ . Entonces,  $b \in X$ .

**Demostración:** Supongamos que  $b \notin X$ , entonces  $b \in A - X$  y, por lo tanto,  $g(b) \in g[A - X]$ . Entonces, de las hipótesis  $g[A - X] = B - f[X]$  y  $f(a) = g(b)$ , tenemos que  $f(a) \in B - f[X]$ . También, de la hipótesis  $a \in X$  tenemos que  $f(a) \in f[X]$ . Por lo tanto, de  $f(a) \in B - f[X]$  y  $f(a) \in f[X]$  obtenemos una contradicción. □

**lemma disj-lemma1:** assumes  $(f' X) = g' (-X)$  and  $f a = g b$  and  $a \in X$

shows  $b \in X$

**proof** (rule ccontr)

```

assume  $b \notin X$  show False
proof –
  let  $?y = g\ b$ 
  have  $?y = g\ b$  by (rule-tac refl)
  moreover
  from  $\langle b \notin X \rangle$  have  $b \in -X$  by simp
  ultimately have  $\exists b \in -X. ?y = g\ b$  by (rule bexI)
  hence  $?y \in g\ '(-X)$  by (simp add: image-def)
  with assms(1) have  $?y \in -(f\ 'X)$  by simp
  with  $\langle f\ a = g\ b \rangle$  have  $f\ a \in -(f\ 'X)$  by simp
  hence  $f\ a \notin f\ 'X$  by simp
  moreover
  from  $\langle a \in X \rangle$  have  $f\ a \in f\ 'X$  by blast
  ultimately show False by contradiction
qed
qed

```

Para la demostración de este lema hemos utilizado, el método de prueba

$$\bullet \frac{\frac{\neg P}{False}}{P} \quad (\text{ccontr})$$

la regla de inferencia de la teoría de conjuntos

$$\bullet \frac{P\ x \quad x \in A}{\exists x \in A. P\ x} \quad (\text{bexI})$$

y el lema de la teoría de conjuntos

$$\bullet f\ 'A \equiv \{y \mid \exists x \in A. y = f\ x\} \quad (\text{image-def})$$

**Lema 4.2.2 (sur-if-then-else)** Sean  $f : A \rightarrow B$ ,  $g : A \rightarrow B$  y  $X \subseteq A$ . Supongamos que  $B - f[X] = g[A - X]$ , entonces la función  $h : A \rightarrow B$  definida por,

$$h(x) = \begin{cases} f(x), & \text{si } x \in X \\ g(x), & \text{si } x \in A - X \end{cases}$$

es sobreyectiva.

**Demostración:** Sea  $y \in B$ . Veamos que existe  $x \in A$  tal que  $y = h(x)$ . Consideremos dos casos: (a)  $y \in f[X]$ , (b)  $y \in B - f[X]$ .

(a) Supongamos que  $y \in f[X]$ . Entonces existe  $x \in X$  tal que  $y = f(x)$ , luego por definición de  $h$ ,  $y = h(x)$ .

(b) Supongamos que  $y \in B - f[X]$ . Entonces, por hipótesis,  $y \in g[A - X]$ , luego existe  $x \in A - X$  tal que  $y = g(x)$ , por lo tanto, por definición de  $h$ ,  $y = h(x)$ . □

**lemma surj-if-then-else1:**

**assumes**  $-(f' X) = g' (-X)$  **shows** *surj*  $(\lambda z. \text{if } z \in X \text{ then } f z \text{ else } g z)$

**proof** (*unfold surj-def*)

**let**  $?h = \lambda z. \text{if } z \in X \text{ then } f z \text{ else } g z$

**show**  $\forall y. \exists x. y = ?h(x)$

**proof**

**fix**  $y$

**show**  $\exists x. y = ?h(x)$

**proof** *cases*

**assume**  $y \in (f' X)$

**hence**  $\exists x \in X. y = f x$  **by** (*simp add:image-def*)

**hence**  $\exists x \in X. y = ?h(x)$  **by** *simp*

**thus**  $\exists x. y = ?h(x)$  **by** *blast*

**next**

**assume**  $y \notin (f' X)$

**hence**  $y \in -(f' X)$  **by** *simp*

**with** *assms* **have**  $y \in g' (-X)$  **by** *simp*

**hence**  $\exists x \in -X. y = g x$  **by** (*simp add:image-def*)

**hence**  $\exists x \in -X. y = ?h(x)$  **by** *simp*

**thus**  $\exists x. y = ?h(x)$  **by** *blast*

**qed**

**qed**

**qed**

En la demostración del lema anterior usamos el método de prueba *unfold* con la definición de función sobreyectiva como argumento

- $\text{surj } f \equiv \forall y. \exists x. y = f x$  (*surj-def*)

**Lema 4.2.3 (bij-if-then-else)** Sean  $f : A \rightarrow B$ ,  $g : A \rightarrow B$  y  $X \subseteq A$ . Se define la función  $f_X : X \rightarrow f[X]$  por,  $f_X(x) = f(x)$  para todo  $x \in X$ ; de la misma forma se define la función  $g_{A-X} : A - X \rightarrow g[A - X]$  por,  $g_{A-X}(x) = g(x)$  para todo  $x \in A - X$ .

Supongamos que  $f_X, g_{A-X}$  son inyectivas y  $B - f[X] = g[A - X]$ , entonces la función  $h : A \rightarrow B$  definida por,

$$h(x) = \begin{cases} f(x), & \text{si } x \in X \\ g(x), & \text{si } x \in A - X \end{cases}$$

es inyectiva y sobreyectiva.

**Demostración:** Mostremos que  $h$  es inyectiva. Sean  $x, y$  tales que  $h(x) = h(y)$ . Para demostrar que  $x = y$ , consideremos los siguientes casos: (a)  $x \in X, y \in X$  (b)  $x \in X, y \in A - X$  (c)  $x \in A - X, y \in X$  (d)  $x \in A - X, y \in A - X$ .

(a) Si  $x \in X, y \in X$ , entonces  $h(x) = f(x) = f_X(x)$  y  $h(y) = f(y) = f_X(y)$ , luego  $f_X(x) = f_X(y)$ . Por lo tanto,  $x = y$  ya que por hipótesis  $f_X$  es inyectiva.

(b) Si  $x \in X, y \in A - X$ , entonces  $h(x) = f(x)$  y  $h(y) = g(y)$ , luego  $f(x) = g(y)$ . De aquí, por el lema 4.2.1, se concluye que  $y \in X$ . De esta forma tenemos que  $y \in A - X$  y  $y \in X$ , lo cual es falso; de esto último deducimos  $x = y$ .

(c) Si  $x \in A - X, y \in X$ , entonces  $h(x) = g(x)$  y  $h(y) = f(y)$ , luego  $g(x) = f(y)$ . De aquí, por el lema ??, se concluye que  $x \in X$ . De esta forma tenemos que  $x \in A - X$  y  $x \in X$ , lo cual es falso; de esto último deducimos  $x = y$ .

(d) Si  $x \in A - X, y \in A - X$ , entonces  $h(x) = g(x) = g_{A-X}(x)$  y  $h(y) = g(y) = g_{A-X}(y)$ , luego  $g_{A-X}(x) = g_{A-X}(y)$ . Por lo tanto,  $x = y$  ya que por hipótesis  $g_{A-X}$  es inyectiva.

Por último, por el lema 4.2.2, se tiene que  $h$  es sobreyectiva. □

**lemma** *bij-if-then-else1*:

**assumes** *hip1*: *inj-on*  $f X$  **and** *hip2*: *inj-on*  $g (- X)$  **and** *hip3*:  $- f' X = g' (- X)$  **and**

*hip4*:  $h = (\lambda z. \text{if } z \in X \text{ then } f z \text{ else } g z)$

**shows** *inj*  $h \wedge$  *surj*  $h$

**proof** — rule *conjI*

**show** *inj*  $h$

**proof** (*unfold inj-on-def*)

**show**  $\forall x \in UNIV. \forall y \in UNIV. h x = h y \longrightarrow x = y$

**proof**

**fix**  $x$

**show**  $\forall y \in UNIV. h x = h y \longrightarrow x = y$

**proof** *cases*

**assume**  $x \in X$

**show**  $\forall y \in UNIV. h x = h y \longrightarrow x = y$

**proof**

**fix**  $y$

**show**  $h x = h y \longrightarrow x = y$

```

proof cases
  assume  $y \in X$ 
  show  $h\ x = h\ y \longrightarrow x = y$ 
  proof — rule impI
    assume  $h\ x = h\ y$  show  $x = y$ 
    proof —
      from  $\langle x \in X \rangle$  and hip4 have  $f\ x = h\ x$  by simp
      also have  $\dots = h\ y$  using  $\langle h\ x = h\ y \rangle$  by simp
      also from  $\langle y \in X \rangle$  and hip4 have  $\dots = f\ y$  by simp
      finally have  $f\ x = f\ y$  by simp
      with hip1 and  $\langle x \in X \rangle$  and  $\langle y \in X \rangle$  show  $x = y$  by (simp add: inj-on-def)
    qed
  qed
next
  assume  $y \notin X$ 
  show  $h\ x = h\ y \longrightarrow x = y$ 
  proof — rule impI
    assume  $h\ x = h\ y$  show  $x = y$ 
    proof —
      from  $\langle x \in X \rangle$  and hip4 have  $f\ x = h\ x$  by simp
      also have  $\dots = h\ y$  using  $\langle h\ x = h\ y \rangle$  by simp
      also from  $\langle y \notin X \rangle$  and hip4 have  $\dots = g\ y$  by simp
      finally have  $f\ x = g\ y$  by simp
      with hip3 and  $\langle x \in X \rangle$  have  $y \in X$  by (simp only: disj-lemma1)
      with  $\langle y \notin X \rangle$  have False by contradiction
      thus  $x = y$  by simp
    qed
  qed
qed
next
  assume  $x \notin X$ 
  show  $\forall y \in UNIV. h\ x = h\ y \longrightarrow x = y$ 
  proof
    fix  $y$ 
    show  $h\ x = h\ y \longrightarrow x = y$ 
    proof cases
      assume hip11:  $y \in X$ 
      show  $h\ x = h\ y \longrightarrow x = y$ 
      proof — rule impI
        assume  $h\ x = h\ y$  show  $x = y$ 
        proof —
          from  $\langle x \notin X \rangle$  and hip4 have  $g\ x = h\ x$  by simp

```

```

    also have ... = h y using ⟨h x = h y⟩ by simp
    also from ⟨y ∈ X⟩ and hip4 have ... = f y by simp
    finally have f y = g x by simp
    with hip3 and ⟨y ∈ X⟩ have x ∈ X by (simp only: disj-lemma1)
    with ⟨x ∉ X⟩ have False by contradiction
    thus x = y by simp
  qed
  qed
next
  assume y ∉ X
  show h x = h y ⟶ x = y
  proof — rule impI
    assume h x = h y show x = y
    proof —
      from ⟨x ∉ X⟩ and hip4 have g x = h x by simp
      also have ... = h y using ⟨h x = h y⟩ by simp
      also from ⟨y ∉ X⟩ and hip4 have ... = g y by simp
      finally have g x = g y by simp
      with hip2 and ⟨x ∉ X⟩ and ⟨y ∉ X⟩ show x = y by (simp add: inj-on-def)
    qed
  qed
  qed
  qed
  qed
  qed
  from hip3 and hip4 show surj h by (simp only: surj-if-then-else1)
qed

```

Tenemos las siguientes dos nuevas reglas aplicadas por el método *rule* en la demostración anterior

$$\bullet \frac{P \quad Q}{P \wedge Q} \quad (\text{conjI})$$

$$\bullet \frac{P}{P \longrightarrow \overline{Q}} \quad (\text{impI})$$

Además se usaron los métodos *unfold* y *simp* con la definición de función inyectiva

$$\bullet \text{inj-on } f A \equiv \forall x \in A. \forall y \in A. f x = f y \longrightarrow x = y \quad (\text{inj--on-def})$$



**Lema 4.2.4 (decomposition)** Dadas las funciones  $f : A \rightarrow B$  y  $g : B \rightarrow A$ , existe  $X$  tal que  $X = A - g[B - f[X]]$ .

**Demostración:** Sea  $\wp(A)$  el conjunto potencia de  $A$ . Para la demostración del lema, basta con probar que la función  $F : \wp(A) \rightarrow \wp(A)$  definida por,  $F(W) = A - g[B - f[W]]$  para todo  $W \subseteq A$ , tiene un punto fijo. Por el Teorema de Knaster-Tarski, es suficiente mostrar que la función  $F$  preserva el orden en el retículo completo  $(\wp(A), \subseteq)$ .

Sean  $U, V$  subconjuntos de  $A$ , con  $U \subseteq V$ . Entonces  $f[U] \subseteq f[V]$ , luego  $B - f[V] \subseteq B - f[U]$ , por lo tanto  $A - (B - f[U]) \subseteq A - (B - f[V])$ , es decir,  $F(U) \subseteq F(V)$ . □

**lemma decomposition1:**  $\exists X. X = - (g' (- (f' X)))$

**proof** –

**let**  $?F = (\lambda X. - g' (- (f' X)))$

**show**  $\exists X. X = ?F X$

**proof** –

**have** *mono*: *mono*  $?F$

**proof** (*unfold mono-def*)

**show**  $\forall A B. A \subseteq B \longrightarrow ?F A \subseteq ?F B$

**proof**

**fix**  $A$

**show**  $\forall B. A \subseteq B \longrightarrow ?F A \subseteq ?F B$

**proof**

**fix**  $B$

**show**  $A \subseteq B \longrightarrow ?F A \subseteq ?F B$

**proof**

**assume** *subconjunto*:  $A \subseteq B$

**show**  $?F A \subseteq ?F B$

**proof** –

**have**  $f' A \subseteq f' B$

**proof** (*rule subsetI*)

**fix**  $y$

**assume** *hip1*:  $y \in f' A$

**show**  $y \in f' B$

**proof** –

**from** *hip1* **have**  $\exists x \in A. y = f x$  **by** (*simp add: image-def*)

**with** *subconjunto* **have**  $\exists x \in B. y = f x$  **by** *blast*

**thus**  $y \in f' B$  **by** (*simp add: image-def*)

**qed**

**qed**

**hence** *menor*:  $(-f' B) \subseteq (-f' A)$  **by** *blast*

```

have  $g'(-f' B) \subseteq g'(-f' A)$ 
proof –
  let  $?C = -f' B$  let  $?D = -f' A$ 
  show  $(g' ?C) \subseteq (g' ?D)$ 
  proof (rule subsetI)
    fix  $y$ 
    assume  $hip1: y \in g' ?C$ 
    show  $y \in g' ?D$ 
    proof –
      from  $hip1$  have  $\exists x \in ?C. y = g x$  by (simp add: image-def)
      with  $menor$  have  $\exists x \in ?D. y = g x$  by blast
      thus  $y \in g' ?D$  by (simp add: image-def)
    qed
  qed
qed
hence  $-g'(-f' A) \subseteq -g'(-f' B)$  by blast
thus  $?F A \subseteq ?F B$  by simp
qed
qed
qed
qed
qed
from mono have  $lfp ?F = ?F (lfp ?F)$  by (rule lfp-unfold)
thus  $\exists X. X = ?F X$  by (rule exI)
qed
qed

```

En la demostración de este lema hemos usado la definición de función monótona

- $mono\ f = (\forall x\ y. x \leq y \longrightarrow f\ x \leq f\ y)$  (*mono-def*)

y también se utilizaron la reglas de inferencia

- $$\frac{\bigwedge x. \frac{x \in A}{x \in B}}{A \subseteq B} \quad (*subsetI*)$$
- $$\frac{mono\ f}{lfp\ f = f\ (lfp\ f)} \quad (*lfp-unfold*)$$

En la demostración del lema anterior se mostró explícitamente que la función  $F$  es monótona. Sin embargo, la prueba se puede hacer automáticamente como se muestra a continuación.

```

lemma decomposition1a:  $\exists X. X = - (g' (- (f' X)))$ 
proof –
  let ?F =  $(\lambda X. - g' (- f' X))$ 
  show  $\exists X. X = ?F X$ 
  proof –
    have mono: mono ?F
    proof (unfold mono-def)
      show  $\forall A B. A \subseteq B \longrightarrow ?F A \subseteq ?F B$  by auto
    qed
  from mono have lfp ?F = ?F (lfp ?F) by (rule lfp-unfold)
  thus  $\exists X. X = ?F X$  by (rule exI)
qed
qed

```

Una versión más simplificada de la demostración del mismo lema es

```

lemma decomposition1b:  $\exists X. X = - (g' (- (f' X)))$ 
proof — rule exI
  let ?F =  $(\lambda X. - g' (- f' X))$ 
  have mono ?F by (unfold mono-def, auto)
  thus lfp ?F = ?F (lfp ?F) by (rule lfp-unfold)
qed

```

**Teorema 4.2.5 (El Teorema de Schröder-Bernstein)** Si  $f : A \rightarrow B$  y  $g : B \rightarrow A$  son funciones inyectivas, entonces existe una función biyectiva  $h : A \rightarrow B$ .

**Demostración:** En lo que sigue usamos el lema 4.2.4 de tal manera que se cumplan las hipótesis del lema 4.2.2 y así construir una función  $h$  biyectiva.

Sea  $X$  tal  $X = A - g[B - f[X]]$ . Entonces,  
 $A - X = A - (A - g[B - f[X]]) = g[B - f[X]]$ .

Ahora, consideremos la función  $f_X : X \rightarrow f[X]$  definida por,  $f_X(x) = f(x)$  para todo  $x \in X$ . Entonces  $f_X$  es inyectiva puesto que  $f$  es inyectiva.

De igual forma, definimos la función  $g_{B-f[X]} : B - f[X] \rightarrow g[B - f[X]]$  por,  $g_{B-f[X]}(x) = g(x)$  para todo  $x \in B - f[X]$ . Puesto que  $g$  es inyectiva,  $g_{B-f[X]}$  es biyectiva, es decir, la función  $g_{B-f[X]} : B - f[X] \rightarrow A - X$  es biyectiva y, por lo tanto existe la función inversa de  $g_{B-f[X]}$ ,  $(g_{B-f[X]})^{-1} : A - X \rightarrow B - f[X]$  definida por,  $(g_{B-f[X]})^{-1}(x) = g^{-1}(x)$  para  $x \in A - X$ . Además,  $(g_{B-f[X]})^{-1}$  es biyectiva, y por lo tanto inyectiva.

Por último, de  $A - X = g[B - f[X]]$ , obtenemos  $(g_{B-f[X]})^{-1}[A - X] = B - f[X]$ .

De lo anterior, se concluye por el lema 4.2.2 que la función  $h : A \rightarrow B$  definida por

$$h(x) = \begin{cases} f(x) & \text{si } x \in X \\ (g_{B-f[X]})^{-1}(x) & \text{si } x \in A - X \end{cases}$$

es biyectiva. □

**theorem** *Schroeder-Bernstein1:*

**fixes**  $f :: 'a \Rightarrow 'b$  **and**  $g :: 'b \Rightarrow 'a$

**assumes** *inyectiva-f: inj f* **and** *inyectiva-g: inj g*

**shows**  $\exists h :: 'a \Rightarrow 'b. \text{inj } h \wedge \text{surj } h$

**proof** –

**from** *decomposition1* [**where**  $f=f$  **and**  $g=g$ , *THEN exE*] **obtain**  $x$  **where**  $x: x = - g' (- f' x)$ .

**show**  $\exists h :: 'a \Rightarrow 'b. \text{inj } h \wedge \text{surj } h$

**proof**

**let**  $?h = (\lambda z. \text{if } z \in x \text{ then } f z \text{ else } \text{inv } g z) :: 'a \Rightarrow 'b$

**show**  $\text{inj } ?h \wedge \text{surj } ?h$

**proof** (*rule bij-if-then-else1* [**where**  $X = x$  **and**  $f = f$  **and**  $g = \text{inv } g$  **and**

$h = (\lambda z. \text{if } z \in x \text{ then } f z \text{ else } \text{inv } g z) :: 'a \Rightarrow 'b$ ])

**show** *inj-on f x*

**proof** –

**have**  $x \subseteq \text{UNIV}$  **by** (*rule subset-UNIV*)

**with** *inyectiva-f* **show** *inj-on f x* **by** (*rule subset-inj-on*)

**qed**

**show** *inj-on (inv g) (- x)*

**proof** –

**from**  $x$  **have**  $- x = - ( - (g' (- (f' x))) )$  **by** *simp*

**hence**  $- x \subseteq \text{range } g$  **by** *blast*

**thus** *inj-on (inv g) (- x)* **by** (*rule inj-on-inv*)

**qed**

**show**  $- (f' x) = (\text{inv } g)' (- x)$

**proof** –

**from**  $x$  **have**  $- x = - ( - (g' (- (f' x))) )$  **by** *simp*

**hence**  $(\text{inv } g)' (- x) = (\text{inv } g)' (g' (- (f' x)))$  **by** *simp*

**with** *inyectiva-g* **show**

$- (f' x) = (\text{inv } g)' (- x)$  **by** (*simp only: inv-image-comp[symmetric]*)

**qed**

**show**

$?h = ((\lambda z. \text{if } z \in x \text{ then } f z \text{ else } \text{inv } g z) :: 'a \Rightarrow 'b)$  **by** (*rule-tac refl*)

**qed**

**qed**

**qed**

En la demostración del teorema anterior hemos usado las siguientes reglas de in-

ferencia

- $A \subseteq UNIV$  (subset-UNIV)
- $\frac{inj-on\ f\ B \quad A \subseteq B}{inj-on\ f\ A}$  (subset-inj-on)
- $\frac{A \subseteq range\ f}{inj-on\ (inv\ f)\ A}$  (inj-on-inv)
- $\frac{inj\ f}{inv\ f'\ f'\ X = X}$  (inv-image-comp)

También hemos utilizado los atributos *where*, *OF* y *THEN*, que permiten derivar propiedades nuevas a partir de otras, es decir, el uso de estas directivas facilitan la presentación de la prueba usando un razonamiento hacia adelante.



# Capítulo 5

## Teoremas básicos de la teoría grupos

En este capítulo se ilustra cómo se emplea el razonamiento ecuacional y el principio de inducción matemática en Isar para demostrar algunas propiedades básicas de la teoría de grupos comparadas con las que se presentan en los textos de matemáticas, por ejemplo en [2].

### 5.1 Definición clásica de grupo y algunas propiedades

**Definición 5.1.1** La estructura  $(G, *, 1, (\cdot)^{-1})$  es un **grupo** si  $G$  es un conjunto,  $1 \in G$ ,  $\cdot$  es una operación en  $G$  y  $(\cdot)^{-1} : G \rightarrow G$  tales que se cumplen las siguientes condiciones:

(A1) *Asociatividad:*  $(x * y) * z = x * (y * z)$ , para todo  $x, y, z \in G$ .

(A2) *Neutro por la izquierda:*  $1 * x = x$  para cualquier  $x \in G$ .

(A3) *Inverso por la izquierda:*  $x^{-1} * x = 1$ , para todo  $x \in G$ .

En Isar se formaliza la clase de los grupos como sigue

**consts**

*one* :: 'a

*inv* :: 'a  $\Rightarrow$  'a

**axclass**

*group* < *times*

*group-assoc*:  $(x * y) * z = x * (y * z)$

*group-left-one*:  $one * x = x$

*group-left-inv*:  $inv\ x * x = one$

donde *times* es la clase de los tipos donde está definida la operación binaria  $*$ .

**Teorema 5.1.2 (Inverso por la derecha)**  $x * x^{-1} = 1$ , para todo  $x \in G$ .

**Demostración:**

$$\begin{aligned}
 x * x^{-1} &= 1 * (x * x^{-1}) && \text{[por A2]} \\
 &= (1 * x) * x^{-1} && \text{[por A1]} \\
 &= (((x^{-1})^{-1} * x^{-1}) * x) * x^{-1} && \text{[por A3]} \\
 &= ((x^{-1})^{-1} * (x^{-1} * x)) * x^{-1} && \text{[por A1]} \\
 &= ((x^{-1})^{-1} * 1) * x^{-1} && \text{[por A2]} \\
 &= (x^{-1})^{-1} * (1 * x^{-1}) && \text{[por A1]} \\
 &= (x^{-1})^{-1} * x^{-1} && \text{[por A2]} \\
 &= 1 && \text{[por A3]}
 \end{aligned}$$

□

**theorem** *group-right-inv*:

**fixes**  $x :: 'a::group$

**shows**  $x * inv\ x = one$

**proof** –

**have**  $x * inv\ x = one * (x * inv\ x)$  **by** (*simp only: group-left-one*)

**also have**  $\dots = one * x * inv\ x$  **by** (*simp only: group-assoc*)

**also have**  $\dots = inv\ (inv\ x) * inv\ x * x * inv\ x$  **by** (*simp only: group-left-inv*)

**also have**  $\dots = inv\ (inv\ x) * (inv\ x * x) * inv\ x$  **by** (*simp only: group-assoc*)

**also have**  $\dots = inv\ (inv\ x) * one * inv\ x$  **by** (*simp only: group-left-inv*)

**also have**  $\dots = inv\ (inv\ x) * (one * inv\ x)$  **by** (*simp only: group-assoc*)

**also have**  $\dots = inv\ (inv\ x) * inv\ x$  **by** (*simp only: group-left-one*)

**also have**  $\dots = one$  **by** (*simp only: group-left-inv*)

**finally show** *?thesis* .

**qed**

**Teorema 5.1.3 (Neutro por la derecha)**  $x * 1 = x$  para cualquier  $x \in G$ .

**Demostración:**

$$\begin{aligned}
 x * 1 &= x * (x^{-1} * x) && \text{[por A3]} \\
 &= (x * x^{-1}) * x && \text{[por A1]} \\
 &= 1 * x && \text{[por 5.1.2]} \\
 &= x && \text{[por A2]}
 \end{aligned}$$

□

**theorem** *group-right-one*:

**fixes**  $x :: 'a::group$

**shows**  $x * one = x$

**proof** –

**have**  $x * one = x * (inv\ x * x)$  **by** (*simp only: group-left-inv*)



**also have** ... =  $x * inv\ x * x$  **by** (simp only: group-assoc)  
**also have** ... =  $one * x$  **by** (simp only: group-right-inv)  
**also have** ... =  $x$  **by** (simp only: group-left-one)  
**finally show** ?thesis .  
**qed**

**Teorema 5.1.4 (Unicidad del elemento neutro)** Sean  $e, x \in G$  tales que  $e * x = x$ . Entonces  $1 = e$ .

**Demostración:** Sean  $e, x \in G$  tales que

$$e * x = x \quad (\text{Hip.})$$

Entonces,

$$\begin{aligned}
 1 &= x * x^{-1} && \text{[por 5.1.2]} \\
 &= (e * x) * x^{-1} && \text{[por Hip.]} \\
 &= e * (x * x^{-1}) && \text{[por A1]} \\
 &= e * 1 && \text{[por 5.1.2]} \\
 &= e && \text{[por 5.1.3]}
 \end{aligned}$$

□

**theorem** group-one-equality:

**fixes**  $e :: 'a::group$

**assumes**  $e * x = x$

**shows**  $one = e$

**proof** –

**have**  $one = x * inv\ x$  **by** (simp only: group-right-inv)  
**also have** ... =  $(e * x) * inv\ x$  **using**  $(e * x = x)$  **by** simp  
**also have** ... =  $e * (x * inv\ x)$  **by** (simp only: group-assoc)  
**also have** ... =  $e * one$  **by** (simp only: group-right-inv)  
**also have** ... =  $e$  **by** (simp only: group-right-one)  
**finally show** ?thesis .

**qed**

**Teorema 5.1.5 (Unicidad del elemento inverso)** Sean  $x, x' \in G$  tales que  $x' * x = 1$ . Entonces  $x^{-1} = x'$ .

**Demostración:** Sean  $x, x' \in G$  tales que

$$x' * x = 1 \quad (\text{Hip.})$$

Entonces,

$$\begin{aligned}
x^{-1} &= 1 * x^{-1} && \text{[por A2]} \\
&= (x' * x) * x^{-1} && \text{[por Hip.]} \\
&= x' * (x * x^{-1}) && \text{[por A1]} \\
&= x' * 1 && \text{[por 5.1.2]} \\
&= x' && \text{[por 5.1.3]}
\end{aligned}$$

□

**theorem** *group-inv-equality*:

**fixes**  $x :: 'a::group$

**assumes**  $x' * x = one$

**shows**  $inv\ x = (x'::'a::group)$

**proof** –

**have**  $inv\ x = one * inv\ x$  **by** (*simp only: group-left-one*)

**also have**  $... = (x' * x) * inv\ x$  **using**  $(x' * x = one)$  **by** *simp*

**also have**  $... = x' * (x * inv\ x)$  **by** (*simp only: group-assoc*)

**also have**  $... = x' * one$  **by** (*simp only: group-right-inv*)

**also have**  $... = x'$  **by** (*simp only: group-right-one*)

**finally show** *?thesis* .

**qed**

**Teorema 5.1.6 (Inverso del producto)**  $(x * y)^{-1} = y^{-1} * x^{-1}$ .

**Demostración:** Por el teorema 5.1.5, basta probar que

$$(y^{-1} * x^{-1}) * (x * y) = 1 \tag{1}$$

La demostración de (1) es

$$\begin{aligned}
(y^{-1} * x^{-1}) * (x * y) &= y^{-1} * (x^{-1} * (x * y)) && \text{[por A1]} \\
&= y^{-1} * ((x^{-1} * x) * y) && \text{[por A1]} \\
&= y^{-1} * (1 * y) && \text{[por A3]} \\
&= y^{-1} * y && \text{[por A2]} \\
&= 1 && \text{[por A3]}
\end{aligned}$$

□

**theorem** *group-inv-times*:

**fixes**  $x :: 'a::group$

**shows**  $inv\ (x * y) = inv\ y * inv\ x$

**proof** (*rule group-inv-equality*)

**show**  $(inv\ y * inv\ x) * (x * y) = one$

**proof** –

**have**  $(inv\ y * inv\ x) * (x * y) = (inv\ y) * ((inv\ x) * x) * y$  **by** (*simp only: group-assoc*)

**also have**  $... = (inv\ y * one) * y$  **by** (*simp only: group-left-inv*)

**also have**  $... = inv\ y * y$  **by** (*simp only: group-right-one*)

**also have**  $... = one$  **by** (*simp only: group-left-inv*)

```

finally show ?thesis .
qed
qed

```

El estilo de prueba usado en los dos teoremas anteriores se corresponde a la presentación dada en un curso introductorio de álgebra. La técnica básica es formar una cadena de ecuaciones, obtenidas y simplificadas por medio de reglas apropiadas. Los detalles lógicos básicos del razonamiento ecuacional son dejados implícitos. En lo que sigue se demuestran otras propiedades de las que mostramos sólo las demostraciones en Isar.

**Teorema 5.1.7 (Inverso del inverso)**  $(x^{-1})^{-1} = x$ .

```

theorem inv-inv:
  fixes x :: 'a::group
  shows inv (inv x) = x
proof (rule group-inv-equality)
  show x * inv x = one by (simp only: group-right-inv)
qed

```

**Teorema 5.1.8** La inversa es inyectiva; es decir, para todo  $x, y$  si  $x^{-1} = y^{-1}$ , entonces  $x = y$ .

```

theorem inv-inject:
  fixes x :: 'a::group
  assumes inv x = inv y
  shows x = y
proof -
  have x = x * one by (simp only: group-right-one)
  also have ... = x * (inv y * y) by (simp only: group-left-inv)
  also have ... = x * (inv x * y) using ⟨inv x = inv y⟩ by simp
  also have ... = (x * inv x) * y by (simp only: group-assoc)
  also have ... = one * y by (simp only: group-right-inv)
  also have ... = y by (simp only: group-left-one)
  finally show ?thesis .
qed

```

**Teorema 5.1.9** Sean  $a$  y  $b$  elementos del grupo  $G$ . Si  $a * x = b$ , entonces  $x = a^{-1} * b$ .

```

theorem soluc-ecuac:
  fixes a :: 'a::group
  assumes a * x = b

```

**shows**  $x = \text{inv } a * b$

**proof**–

**have**  $x = \text{one} * x$  **by** (*simp only: group-left-one*)

**also have**  $\dots = (\text{inv } a * a) * x$  **by** (*simp only: group-left-inv*)

**also have**  $\dots = \text{inv } a * (a * x)$  **by** (*simp only: group-assoc*)

**also have**  $\dots = \text{inv } a * b$  **using**  $\langle a * x = b \rangle$  **by** *simp*

**finally show** ?thesis .

**qed**

**Teorema 5.1.10** *Sea  $a$  un elemento del grupo  $G$ . Si  $a * x = a * y$ , entonces  $x = y$ .*

**theorem cancelativa:**

**fixes**  $a :: 'a::\text{group}$

**assumes**  $a*x = a*y$

**shows**  $x = y$

**proof**–

**have**  $x = \text{one} * x$  **by** (*simp only: group-left-one*)

**also have**  $\dots = (\text{inv } a * a)*x$  **by** (*simp only: group-left-inv*)

**also have**  $\dots = \text{inv } a * (a*x)$  **by** (*simp only: group-assoc*)

**also have**  $\dots = \text{inv } a * (a*y)$  **using**  $\langle a*x = a*y \rangle$  **by** *simp*

**also have**  $\dots = (\text{inv } a * a)*y$  **by** (*simp only: group-assoc*)

**also have**  $\dots = \text{one} * y$  **by** (*simp only: group-left-inv*)

**also have**  $\dots = y$  **by** (*simp only: group-left-one*)

**finally show** ?thesis .

**qed**

Usando el teorema 5.1.9, tenemos otra forma de demostrar la ley cancelativa.

**theorem cancelativa1:**

**fixes**  $a :: 'a::\text{group}$

**assumes**  $a*x = a*y$

**shows**  $x = y$

**proof**–

**from**  $\langle a*x = a*y \rangle$  **have**  $x = \text{inv } a * (a*y)$  **by** (*simp only: soluc-ecuac*)

**also have**  $\dots = (\text{inv } a * a)*y$  **by** (*simp only: group-assoc*)

**also have**  $\dots = \text{one}*y$  **by** (*simp only: group-left-inv*)

**also have**  $\dots = y$  **by** (*simp only: group-left-one*)

**finally show** ?thesis .

**qed**

## 5.2 Combinando el método de deducción natural y el cálculo ecuacional

En esta sección ilustraremos con un ejemplo la forma de integrar en Isar la deducción natural y el razonamiento ecuacional. Para ello, demostramos el siguiente teorema.

**Teorema 5.2.1** *Sea  $G$  un grupo. Si  $x * x = e$  para todo  $x \in G$ , entonces  $x * y = y * x$  para todo  $x, y \in G$ .*

**Demostración:** Sean  $a, b$  elementos de  $G$ , entonces

$$\begin{aligned}
 a * b &= e * (a * b) && [(A3)] \\
 &= (b * b) * (a * b) && [\text{hipótesis}] \\
 &= (b * (e * b)) * (a * b) && [(A3)] \\
 &= (b * ((a * a) * b)) * (a * b) && [\text{hipótesis}] \\
 &= (b * (a * (a * b))) * (a * b) && [(A2)] \\
 &= ((b * a) * (a * b)) * (a * b) && [(A2)] \\
 &= (b * a) * ((a * b) * (a * b)) && [(A2)] \\
 &= (b * a) * e && [\text{hipótesis}] \\
 &= b * a && [(A3)]
 \end{aligned}$$

□

Ahora, tenemos la correspondiente formulación y demostración en Isar del teorema anterior.

**theorem** *orden1:*

**assumes**  $\forall (x::'a::\text{group}). x * x = \text{one}$

**shows**  $\forall (x::'a::\text{group}) y. x * y = y * x$

**proof** — rule allI

**fix**  $a :: 'a::\text{group}$

**show**  $\forall y. a * y = y * a$

**proof** — rule allI

**fix**  $b$

**show**  $a * b = b * a$

**proof** —

**have**  $a * b = \text{one} * (a * b)$  **by** (*simp only: group-left-one*)

**also have**  $\dots = (b * b) * (a * b)$  **using** *assms* **by** *simp* — rule allE

**also have**  $\dots = (b * (\text{one} * b)) * (a * b)$  **by** (*simp only: group-left-one*)

**also have**  $\dots = (b * ((a * a) * b)) * (a * b)$  **using** *assms* **by** *simp* — rule allE

**also have**  $\dots = (b * a) * ((a * b) * (a * b))$  **by** (*simp only: group-assoc*)

**also have**  $\dots = (b * a) * \text{one}$  **using** *assms* **by** *simp* — rule allE

**also have**  $\dots = b * a$  **by** (*simp only: group-right-one*)

**ultimately show**  $a * b = b * a$  **by** *simp*

qed  
qed  
qed

El método de prueba que hemos usado en la demostración anterior es la aplicación de la regla de introducción del cuantificador universal

$$\bullet \frac{\bigwedge x. P x}{\forall x. P x} \quad (allI)$$

Además, el *simplificador* utiliza automáticamente en algunos pasos de la prueba, como se indica arriba, la regla de eliminación del cuantificador universal.

$$\bullet \frac{\forall x. P x \quad \frac{P x}{R}}{R} \quad (allE)$$

### 5.3 Demostraciones por inducción

En esta sección mostramos cómo se utiliza en Isar el principio de inducción matemática, en forma análoga a como se emplea en matemáticas, para la demostración de propiedades sobre conceptos definidos inductivamente. En particular, demostramos algunas propiedades sobre los exponentes en un grupo arbitrario.

**Definición 5.3.1** Sea  $G$  un grupo con elemento identidad  $e$  y  $n \geq 0$  un número natural. Para  $a \in G$  se define la potencia  $n$ -ésima de  $a$ ,  $a^n$ , de la siguiente forma:

$$(P1) \quad a^0 = e.$$

$$(P2) \quad a^{n+1} = a * a^n.$$

Para formalizar en Isar el concepto de potencia, introducimos la clase *power* como una subclase de grupos en donde está definida la función potencia (representada por  $\sim$ ) y verificando las dos propiedades anteriores que definen la potencia de un elemento del grupo.

**consts**

*power* :: 'a  $\Rightarrow$  nat  $\Rightarrow$  'a (**infixr**  $\sim$  80)

**axclass**

```
power < group
group-power-cero: x ~ 0 = (one::'a::group)
group-power-suc: x ~ (Suc n) = x * (x ~ n)
```

En la demostración de las siguientes propiedades sobre los exponentes usamos el método de inducción matemática.

**Teorema 5.3.2** *En un grupo  $G$ ,  $e^n = e$  para todo número natural  $n$ .*

**Demostración:** Lo demostraremos por inducción.

**Base:**  $e^0 = e$  que es verdadera, por (P1).

**Paso de inducción:** Supongamos que  $e^n = e$  es verdadera para  $n$ . Entonces

$$\begin{aligned} e^{n+1} &= e * e^n && \text{[por (P2)]} \\ &= e * e && \text{[por hipótesis]} \\ &= e && \text{[por (A3)]} \end{aligned}$$

Por tanto,  $e^{n+1} = e$ .

□

**theorem power-one1:**

```
one ~ n = (one::'a::power) (is ?P n is ?S n = -)
```

**proof** (induct n)

```
show ?P 0 by (simp only: group-power-cero)
```

**next**

```
fix n assume hip: ?S n = one
```

```
have ?S (n+1) = one * (one ~ n) by (simp add: group-power-suc)
```

```
moreover have ... = one * one by (simp only: group-power-suc)
```

```
moreover have ... = one * one by (simp only: hip)
```

```
moreover have ... = one by (simp only: group-left-one)
```

```
ultimately show ?P (Suc n) by simp
```

**qed**

El teorema puede demostrarse de manera automática como se muestra a continuación.

**theorem power-one2:**  $one \sim n = (one::'a::power)$

**by** (induct n) (simp-all add: group-power-cero group-power-suc group-left-one)

**Teorema 5.3.3** *Sea  $G$  un grupo y  $a \in G$ , entonces  $a^{m+n} = a^m * a^n$  para todo par de números naturales  $m, n$ .*

**Demostración:** Por inducción en  $m$ . Sea  $n$  un número natural y  $P(m)$  la propiedad  $a^{m+n} = a^m * a^n$ .

**Base:**  $P(0)$  es  $a^{0+n} = a^0 * a^n$  que es verdadera ya que

$$\begin{aligned} a^{0+n} &= a^n && \text{[por propiedad de los naturales]} \\ &= e * a^n && \text{[por (A3)]} \\ &= a^0 * a^n && \text{[por (P1)]} \end{aligned}$$

**Paso de inducción:** Supongamos que  $P(m)$  es verdadera. Mostremos que  $P(m+1)$  también lo es

$$\begin{aligned} a^{(m+1)+n} &= a^{(m+n)+1} && \text{[por propiedad de los naturales]} \\ &= a * a^{m+n} && \text{[por (P2)]} \\ &= a * (a^m * a^n) && \text{[por hipótesis]} \\ &= (a * a^m) * a^n && \text{[por (A3)]} \\ &= a^{m+1} * a^n && \text{[por (P2)]} \end{aligned}$$

□

**theorem power-add1:**

$(a::'a::power) \sim (m+n) = (a \sim m) * (a \sim n)$  (is ?P m is ?S m = -)

**proof** (induct m)

**show** ?P 0 by (simp add: group-power-cero group-left-one)

**next**

**fix** m **assume** hip: ?S m = (a ~ m) \* (a ~ n)

**have** ?S (Suc m) = a ~ Suc(m+n) **by** simp

**moreover have** ... = a \* (a ~ (m+n)) **by** (simp only: group-power-suc)

**moreover have** ... = a \* ?S m **by** simp

**moreover have** ... = a \* ((a ~ m) \* (a ~ n)) **by** (simp only: hip)

**moreover have** ... = (a \* (a ~ m)) \* (a ~ n) **by** (simp only: group-assoc)

**moreover have** ... = (a ~ Suc m) \* (a ~ n) **by** (simp only: group-power-suc)

**ultimately show** ?P (Suc m) **by** simp

**qed**

El teorema puede demostrarse de manera automática como se muestra a continuación.

**theorem power-add2:**  $(a::'a::power) \sim (m+n) = (a \sim m) * (a \sim n)$

**by** (induct m) (simp-all add: group-power-cero group-left-one group-power-suc group-assoc)

**Teorema 5.3.4** Sea  $G$  un grupo y  $a \in G$ , entonces  $a^{m*n} = (a^m)^n$  para todo par de números naturales  $m, n$ .

**Demostración:** Por inducción en  $n$ . Sea  $m$  un número natural y  $P(n)$  la propiedad  $a^{m*n} = (a^m)^n$ .

**Base:**  $P(0)$  es  $a^{m*0} = (a^m)^0$  que es verdadera, ya que

$$\begin{aligned} a^{m*0} &= a^0 && \text{[por propiedad de los naturales]} \\ &= e && \text{[por (P1)]} \\ &= (a^m)^0 && \text{[por (P1)]} \end{aligned}$$



**Paso de inducción:** Supongamos que  $P(n)$  es verdadera. Mostremos que  $P(n + 1)$  también lo es.

$$\begin{aligned}
 a^{m*(n+1)} &= a^{m+m*n} && \text{[por propiedad de los naturales]} \\
 &= a^m * a^{m*n} && \text{[por teorema anterior]} \\
 &= a^m * (a^m)^n && \text{[por hipótesis]} \\
 &= (a^m)^{n+1} && \text{[por (P2)]}
 \end{aligned}$$

□

**theorem** *power-mult1:*

$$(a::'a::power)^{\sim}(m * n) = (a \sim m)^{\sim} n \text{ (is ?P n is ?S n = -)}$$

**proof** (*induct n*)

**show** ?P 0 **by** (*simp add: group-power-cero*)

**next**

**fix** n **assume** *hip: ?S n = (a ~ m) ~ n*

**have** ?S (n+1) =  $a^{\sim}(m+m*n)$  **by** (*simp add: power-add1*)

**moreover have** ... =  $(a^{\sim}m) * (a^{\sim}(m*n))$  **by** (*simp only: power-add1*)

**moreover have** ... =  $(a^{\sim}m) * ?S n$  **by** *simp*

**moreover have** ... =  $(a \sim m) * (a^{\sim}m)^{\sim}n$  **by** (*simp only: hip*)

**moreover have** ... =  $(a \sim m)^{\sim} \text{Suc } n$  **by** (*simp only: group-power-suc*)

**ultimately show** ?P (*Suc n*) **by** *simp*

**qed**

El teorema puede demostrarse de manera automática como se muestra a continuación.

**theorem** *power-mult2:*  $(a::'a::power)^{\sim}(m * n) = (a \sim m)^{\sim} n$

**by** (*induct n*) (*simp-all add: group-power-cero power-add2 group-power-suc*)



# Capítulo 6

## Números primos

Con el fin de ilustrar cómo se demuestran en Isar propiedades acerca de números primos, en este capítulo demostramos la siguiente propiedad de los números primos.

*$p$  y  $p^2 + 2$  son números primos si y solamente si  $p = 3$*

Un número natural  $p$  mayor que 1 es primo si y solamente si sus únicos divisores son 1 y  $p$ . En Isar se formaliza este concepto de la siguiente manera,

**definition**

*prime* :: nat  $\Rightarrow$  bool **where**

*prime*  $p \longleftrightarrow (1 < p \wedge (\forall m. m \text{ dvd } p \longrightarrow m = 1 \vee m = p))$

en donde,  $(m \text{ dvd } n) = (\exists k. n = m * k)$ .

Algunas propiedades sobre números utilizadas en la prueba, son enunciadas como lemas.

### 6.1 Propiedades elementales sobre divisibilidad

**Lema 6.1.1** Sean  $a, b$  números naturales. Entonces  $(a + b)^2 = a^2 + 2ab + b^2$

**Demostración:**

$$\begin{aligned} (a + b)^2 &= (a + b)(a + b) && \text{[definición de potencia]} \\ &= (a + b)a + (a + b)b && \text{[propiedad distributiva]} \\ &= aa + ba + ab + bb && \text{[propiedad distributiva]} \\ &= aa + ab + ab + bb && \text{[propiedad conmutativa de la multiplicación]} \\ &= aa + 2ab + bb && \text{[simplificación]} \\ &= a^2 + 2ab + b^2 && \text{[definición de potencia]} \end{aligned}$$

□

**lemma binomio:** fixes  $a::nat$

shows  $(a+b)^2 = a^2 + 2*a*b + b^2$

**proof** –

**have**  $(a + b)^2 = (a + b)*(a + b)$  **by** (rule power2-eq-square)

**also have**  $\dots = ((a + b)*a) + ((a + b)*b)$  **by** (simp only: add-mult-distrib2)

**also have**  $\dots = a*a + b*a + a*b + b*b$  **by** (simp only: add-mult-distrib)

**also have**  $\dots = a*a + a*b + a*b + b*b$  **by** (simp only: mult-commute)

**also have**  $\dots = a*a + 2*a*b + b*b$  **by** simp

**also have**  $\dots = a^2 + 2*a*b + b^2$  **by** (simp only: power2-eq-square)

**finally show** ?thesis **by** simp

**qed**

La demostración anterior se puede escribir en forma abreviada:

**lemma binomio1:** fixes  $a::nat$

shows  $(a+b)^2 = a^2 + 2*a*b + b^2$

**proof** –

**have**  $(a + b)^2 = (a + b)*(a + b)$  **by** (rule power2-eq-square)

**also have**  $\dots = a^2 + 2*a*b + b^2$

**by** (simp add : add-mult-distrib2 add-mult-distrib mult-commute power2-eq-square)

**finally show** ?thesis **by** simp

**qed**

Los lemas utilizados en la demostración anterior son

- $a^2 = a * a$  (power2-eq-square)
- $k * (m + n) = k * m + k * n$  (add-mult-distrib2)
- $(m + n) * k = m * k + n * k$  (add-mult-distrib)
- $a * b = b * a$  (mult-commute)

**Lema 6.1.2** Sean  $a, b, c$  números naturales. Entonces

$$(a + (bc))^2 = a^2 + 2abc + b^2c^2$$

**Demostración:**  $(a + (bc))^2 = a^2 + 2a(bc) + (bc)^2$  [lema 6.1.1]  
 $= a^2 + 2a(bc) + b^2c^2$  [propiedad de los exponentes]

□

**lemma simplificacion:** fixes  $a::nat$

shows  $(a + (b*c))^2 = a^2 + 2*a*b*c + (b^2)*(c^2)$

**proof** –

**have**  $(a + (b*c))^2 = a^2 + 2*a*(b*c) + (b*c)^2$  **by** (rule binomio)  
**also have**  $... = a^2 + 2*a*(b*c) + (b^2)*(c^2)$  **by** (simp add: power-mult-distrib)  
**finally show** ?thesis **by** simp  
**qed**

El lema usado en la demostracion anterior es

- $(a * b) ^ n = a ^ n * b ^ n$  (power-mult-distrib)

**Lema 6.1.3** Si  $a$  divide a  $b$  y  $a \neq 1$  y  $a \neq b$ , entonces  $b$  no es un número primo.

**Demostración:** Basta con aplicar la definición de número primo. □

**lemma noprime:** **assumes**  $a \text{ dvd } b$  **and**  $a \neq 1$  **and**  $a \neq b$  **shows**  $\neg \text{prime } b$   
**proof** –  
**have**  $a \text{ dvd } b \wedge a \neq 1 \wedge a \neq b$  **using** *assms* **by** simp  
**hence**  $\exists a. a \text{ dvd } b \wedge a \neq 1 \wedge a \neq b$  **by** (rule exI)  
**thus**  $\neg \text{prime } b$  **by** (simp add: prime-def)  
**qed**

**Lema 6.1.4** Sea  $k$  un número natural. Si  $k \bmod 3 = 1$  ó  $k \bmod 3 = 2$  entonces  $(3 + k)^2 + 2$  no es primo.

**Demostración:** Supongamos que  $k \bmod 3 = 1$ . Entonces, existe  $q$  tal que  $k = 1 + 3q$ . Luego, por el lema 6.1.2 y otras propiedades de los números, tenemos que

$$(3 + k)^2 + 2 = (4 + 3q)^2 = 3(6 + 8q + 3q^2).$$

De esta última ecuación tenemos que existe  $m \neq 1$  tal que  $(3 + k)^2 + 2 = 3m$ . De esta forma, tenemos que 3 divide a  $(3 + k)^2 + 2$  y  $3 \neq (3 + k)^2 + 2$ , además  $3 \neq 1$ . Por lo tanto, por el lema 6.1.3,  $(3 + k)^2 + 2$  no es primo.

Si  $k \bmod 3 = 2$  entonces, de igual forma que en el caso anterior, se concluye que  $(3 + k)^2 + 2$  no es primo. □

**lemma noprimesiduo:** **assumes**  $k \bmod 3 = 1 \vee k \bmod 3 = 2$  **shows**  $\neg \text{prime}((3+k)^2+2)$   
**proof** (rule disjE)  
**assume**  $k \bmod 3 = 1$   
**hence**  $\exists q. k = 1 + q*3$  **by** (rule mod-eqD)  
**then obtain**  $q$  **where**  $k = 1 + q*3$  **by** (rule exE)  
**hence**  $3 + k = 4 + 3*q$  **by** simp

**hence**  $(3+k)^2 = (4 + 3*q)^2$  **by simp**  
**also have**  $... = 4^2 + 2 * 4*(3*q) + 3^2*q^2$  **by (simp add: simplificacion)**  
**also have**  $... = 16 + 24*q + 9*q^2$  **by simp**  
**finally have**  $(3+k)^2 + 2 = 18 + 24*q + 9*q^2$  **by simp**  
**hence ecuacion:**  $(3+k)^2 + 2 = 3*(6 + 8*q + 3*q^2)$  **by simp**  
**hence**  $\exists m. (3+k)^2 + 2 = 3*m$  **by (rule exI)**  
**hence**  $3 \text{ dvd } (3+k)^2 + 2$  **by (simp add: dvd-def)**  
**moreover**  
**have**  $(3::nat) \neq 1$  **by simp**  
**moreover**  
**from ecuacion have**  $3 \neq (3+k)^2 + 2$  **by simp**  
**ultimately show**  $\neg \text{prime}((3+k)^2 + 2)$  **by (rule noprimo)**  
**next**  
**assume**  $k \text{ mod } 3 = 2$   
**hence**  $\exists q. k = 2 + q*3$  **by (rule mod-eqD)**  
**then obtain q where**  $k = 2 + q*3$  **by (rule exE)**  
**hence**  $3 + k = 5 + 3*q$  **by simp**  
**hence**  $(3+k)^2 = (5 + 3*q)^2$  **by simp**  
**also have**  $... = 5^2 + 2 * 5*(3*q) + 3^2*q^2$  **by (simp add: simplificacion)**  
**also have**  $... = 25 + 30*q + 9*q^2$  **by simp**  
**finally have**  $(3+k)^2 + 2 = 27 + 30*q + 9*q^2$  **by simp**  
**hence ecuacion:**  $(3+k)^2 + 2 = 3*(9 + 10*q + 3*q^2)$  **by simp**  
**hence**  $\exists m. (3+k)^2 + 2 = 3*m$  **by (rule exI)**  
**hence**  $3 \text{ dvd } (3+k)^2 + 2$  **by (simp add: dvd-def)**  
**moreover**  
**have**  $(3::nat) \neq 1$  **by simp**  
**moreover**  
**from ecuacion have**  $3 \neq (3+k)^2 + 2$  **by simp**  
**ultimately show**  $\neg \text{prime}((3+k)^2 + 2)$  **by (rule noprimo)**  
**qed**

Para la prueba anterior se utilizó la regla de inferencia

$$\bullet \frac{m \text{ mod } d = r}{\exists q. m = r + q * d} \quad (\text{mod-eqD})$$

**Lema 6.1.5** Sea  $k$  un número natural, entonces

$$k \text{ mod } 3 = 0 \vee k \text{ mod } 3 = 1 \vee k \text{ mod } 3 = 2$$

**Demostración:** Supongamos que  $\neg(k \text{ mod } 3 = 1 \vee k \text{ mod } 3 = 2)$ , entonces  $k \text{ mod } 3 \neq 1$  y  $k \text{ mod } 3 \neq 2$ . Por el teorema del residuo sabemos que,  $0 \leq (k \text{ mod } 3) < 3$ , luego

$k \bmod 3 = 0$ .

□

**lemma residuotres1:** **fixes**  $k::nat$  **shows**  $k \bmod 3 = 0 \vee k \bmod 3 = 1 \vee k \bmod 3 = 2$

**proof** (rule *disjCI*)

**assume**  $\neg(k \bmod 3 = 1 \vee k \bmod 3 = 2)$

**hence**  $k \bmod 3 \neq 1 \wedge k \bmod 3 \neq 2$  **by** *simp*

**thus**  $k \bmod 3 = 0$  **by** *arith*

**qed**

Para la demostración de este lema se ha utilizado la regla de inferencia

$$\bullet \frac{\frac{\neg Q}{P}}{P \vee Q} \quad (\text{disjCI})$$

La demostración anterior se puede hacer utilizando únicamente el método *arith*.

**lemma residuotres:** **fixes**  $k::nat$

**shows**  $k \bmod 3 = 0 \vee k \bmod 3 = 1 \vee k \bmod 3 = 2$  **by** *arith*

**Lema 6.1.6** Sean  $a, b$  números naturales. Si  $a$  divide a  $b$  entonces  $a$  divide a  $a + b$

**Demostración:** Supongamos que  $a$  divide a  $b$ , entonces existe  $k$  tal que  $b = ak$ , de donde,  $a + b = a + ak = a(1 + k)$ . Por lo tanto, existe  $n$  tal que  $a + b = an$ , luego  $a$  divide a  $a + b$ .

□

**lemma dividesuma:** **fixes**  $a::nat$

**assumes**  $a \text{ dvd } b$  **shows**  $a \text{ dvd } (a+b)$

**proof** –

**from**  $\langle a \text{ dvd } b \rangle$  **obtain**  $k$  **where**  $b = a * k$  ..

**hence**  $a+b = a + a*k$  **by** *simp*

**also have**  $... = a*(1 + k)$  **by** (*simp add: add-mult-distrib2*)

**finally have**  $a+b = a*(1 + k)$  **by** *simp*

**hence**  $\exists n. a+b = a*n$  **by** (*rule exI*)

**thus** *?thesis* **by** (*simp add: dvd-def*)

**qed**

**Lema 6.1.7** El número 3 es primo.

**Demostración:** Tenemos que  $3 > 1$ . Mostremos que para todo número natural  $m$ , si  $m$  divide a 3 entonces  $m = 1 \vee m = 3$ .

Sea  $m$  un número natural tal que  $m$  divide a 3. Supongamos que  $m \neq 3$ , probemos que  $m = 1$ .

Puesto que  $3 > 0$  y  $m$  divide a 3 entonces, por propiedades de la divisibilidad  $0 < m \leq 3$  y, como estamos suponiendo que  $m \neq 3$  tenemos que  $0 < m < 3$ , es decir,  $m = 1 \vee m = 2$ ; además se tiene que  $3 = mk$ , para algún  $k$ . De esta igualdad se sigue que no es posible  $m = 2$ , y por lo tanto  $m = 1$ . □

**lemma tresprimo:** *prime 3*

**proof** (*unfold prime-def*)

**have**  $(1::nat) < 3$  **by** *simp*

**moreover**

**have**  $\forall (m::nat). m \text{ dvd } 3 \longrightarrow m = 1 \vee m = 3$

**proof**

**fix**  $m::nat$

**show**  $m \text{ dvd } 3 \longrightarrow m = 1 \vee m = 3$

**proof**

**assume**  $m \text{ dvd } 3$

**show**  $m=1 \vee m = 3$

**proof** (*rule disjCI*)

**assume**  $m \neq 3$

**show**  $m=1$

**proof** –

**have**  $m \neq 0$

**proof**

**assume**  $m=0$

**with**  $\langle m \text{ dvd } 3 \rangle$  **have**  $(3::nat) = 0$  **by** (*simp add: dvd-0-left*)

**thus** *False* **by** *arith*

**qed**

**moreover**

**have**  $m \leq 2$

**proof** –

**have**  $0 < (3::nat)$  **by** *simp*

**with**  $\langle m \text{ dvd } 3 \rangle$  **have**  $m \leq 3$  **by** (*rule dvd-imp-le*)

**with**  $\langle m \neq 3 \rangle$  **show**  $m \leq 2$  **by** *simp*

**qed**

**moreover**

**have**  $m \neq 2$

**proof**

**assume**  $m=2$

**moreover**

**from**  $\langle m \text{ dvd } 3 \rangle$  **have**  $\exists k. 3 = m * k$  **by** (*simp add: dvd-def*)

**moreover**



then obtain  $k$  where  $3 = m*k$  by (rule exE)  
 hence  $3 = 2*k$  using  $\langle m=2 \rangle$  by simp  
 thus False by arith  
 qed  
 ultimately  
 show  $m = 1$  by simp  
 qed  
 qed  
 qed  
 ultimately show  $(1::nat) < 3 \wedge (\forall (m::nat). m \text{ dvd } 3 \longrightarrow m = 1 \vee m = 3)$   
 by (rule conjI)  
 qed

En la demostración anterior utilizamos el lema,

- $0 \text{ dvd } m \implies m = 0$  (dvd-0-left)

y la regla de inferencia

- $$\frac{?k \text{ dvd } ?n \quad 0 < ?n}{?k \leq ?n}$$
 (dvd-imp-le)

**Lema 6.1.8** *El número 11 es primo.*

**Demostración:** Tenemos que  $11 > 1$ . Mostremos que para todo número natural  $m$ , si  $m$  divide a 11 entonces  $m = 1 \vee m = 11$ .

Sea  $m$  un número natural tal que  $m$  divide a 11. Supongamos que  $m \neq 11$ , probemos que  $m = 1$ .

Puesto que  $11 > 0$  y  $m$  divide a 11 entonces, por propiedades de la divisibilidad  $0 < m \leq 11$  y, como estamos suponiendo que  $m \neq 11$  tenemos que  $0 < m < 11$ , es decir,  $m = 1 \vee m = 2 \vee \dots \vee m = 10$ . Por otro lado, se tiene que  $11 = mk$ , para algún  $k$ . Al sustituir en esta ecuación  $m$  por sus valores posibles, concluimos que  $m = 1$ , ya que en cualquier otro caso la igualdad no se cumple.

□

Como lo la prueba anterior, para demostrar a partir de la definición que un número natural  $n > 1$  es primo, hay que mostrar que para cualquier natural  $m$ , si  $2 \leq m < n$  entonces,  $m$  no divide a  $n$ ; esto es, hay que probar que para cualquier natural  $k, n \neq mk$ . Es conocido que no hay un método algebraico elemental, utilizando propiedades de la multiplicación, que sirva para demostrar de manera general esta implicación; En Isar

podemos hacer la demostración por distinción de casos, utilizando propiedades de la aritmética, verificando mecánicamente que para cada valor específico de  $m$  (numeral) se tiene que  $n \neq mk$ . Para esto se define una función que genere los números  $m$  desde 2 hasta  $n - 1$ , posteriormente, utilizando el método *auto*, se reemplaza  $m$  por cada uno de estos valores en la inecuación  $n \neq mk$  y luego, utilizando el método *arith*, se demuestra en cada caso la desigualdad. El número de comprobación de casos se puede reducir teniendo en cuenta que si  $n$  no tiene divisores menores o iguales que  $\sqrt{n}$  tampoco tiene divisores mayores que  $\sqrt{n}$ . En lo que sigue, utilizamos el procedimiento anterior para demostrar que  $n = 11$  es primo.

Definimos la siguiente función "*ListaNumeros i N []*" de forma tal que dados los números naturales  $i, N$  retorna la lista conformada por los números desde  $i$  hasta  $N$ , por ejemplo *ListaNumeros 2 10 []*=[2,3,...,10].

```
function ListaNumeros :: nat ⇒ nat ⇒ nat list ⇒ nat list
where
  ListaNumeros i N L = (if i > N then [] else i#(ListaNumeros (Suc i) N L))
by pat-completeness auto
```

En la definición anterior el método *pat-completeness* es usado para verificar que cada elemento  $x$  del tipo de entrada de la función coincide con por lo menos uno de los patrones que especifican las condiciones que deben cumplir los datos de entrada, y además si coincide con más de un patron, los resultados al sustituir  $x$  en cada fórmula asociada al patron correspondiente, deben ser iguales.

Obsérvese que la función *ListaNumeros* es recursiva general. Para definir una medida que permita probar la terminación del cálculo de los valores de la función, tenemos en cuenta que en cada llamado recursivo la *diferencia* entre  $N$  e  $i$  disminuye, y que la recursión termina cuando  $i$  es mayor que  $N$ . De esta forma, usamos la expresión  $N + 1 - i$  para definir una función de medida. Nótese que, en este caso, el método del *orden lexicográfico* no sirve como medida de terminación ya que ninguno de los argumentos decrece en el llamado recursivo con respecto al tamaño estandar de ordenamiento.

En forma precisa, como se indica en [4], la demostración de terminación es la siguiente

```
termination ListaNumeros
apply (relation measure (λ (i,N,L). N + 1 - i))
apply auto
done
```

La regla de inferencia usada en la prueba es

$$\bullet \frac{wf R \quad \bigwedge i N L. \frac{\neg N < i}{((Suc i, N, L), i, N, L) \in R}}{\forall x. ListaNumeros-dom x} \quad (termination)$$

En donde  $R$  es la relación que se obtiene, a partir de la función predefinida *measure* con argumento la medida  $(\lambda(i, N, L). N + 1 - i)$ , al invocar el método *relation*. Con esta relación específica  $R$ , los dos sub-objetivos que se tienen como premisas en la regla de inferencia, es decir, que  $R$  es bien fundada y que los argumentos de los llamados recursivos decrecen con respecto a la relación, son probados por el método *auto*.

La comprobación del ejemplo es

```
lemma ListaNumeros 2 10 [] = [2,3,4,5,6,7,8,9,10]
by simp
```

En el siguiente lema mostramos que 11 no se puede escribir de la forma  $m * k$  en donde  $m, k$  son números naturales con  $2 \leq m \leq 10$ .

```
lemma diferenteonce: fixes m :: nat
  assumes 2 ≤ m ∧ m ≤ 10 shows 11 ≠ m*k
proof –
  from assms have m ∈ set (ListaNumeros 2 10 []) by auto
  thus ?thesis by (auto,arith+)
qed
```

Ahora, tenemos la correspondiente demostración en Isar de que el número 11 es primo.

```
lemma onceprimo: prime 11
proof (unfold prime-def)
  have (1::nat) < 11 by simp
  moreover
  have  $\forall (m::nat). m \text{ dvd } 11 \longrightarrow m = 1 \vee m = 11$ 
  proof
    fix m::nat
    show m dvd 11  $\longrightarrow$  m = 1  $\vee$  m = 11
    proof
      assume m dvd 11
      hence  $\exists k. 11 = m*k$  by (simp add: dvd-def)
      then obtain k where k: 11 = m*k by (rule exE)
      show m=1  $\vee$  m = 11
      proof (rule disjCI)
        assume m ≠ 11
        show m=1
        proof –
          have m ≠ 0
          proof
            assume m=0
            with (m dvd 11) have (11::nat) =0 by (simp add: dvd-0-left)
            thus False by arith
          qed
        qed
      qed
    qed
  qed
```

```

qed
moreover
have  $m \leq 10$ 
proof -
  have  $0 < (11::nat)$  by simp
  with  $\langle m \text{ dvd } 11 \rangle$  have  $m \leq 11$  by (rule dvd-imp-le)
  with  $\langle m \neq 11 \rangle$  show  $m \leq 10$  by simp
qed
moreover
have  $\neg(2 \leq m \wedge m \leq 10)$ 
proof
  assume  $2 \leq m \wedge m \leq 10$ 
  hence  $\neg(11 = m * k)$  by (rule diferenteonce)
  with  $k$  show False by simp
qed
ultimately show  $m = 1$  by simp
qed
qed
qed
qed
ultimately
show  $(1::nat) < 11 \wedge (\forall (m::nat). m \text{ dvd } 11 \longrightarrow m = 1 \vee m = 11)$ 
by (rule conjI)
qed

```

## 6.2 Teorema principal sobre números primos

**Teorema 6.2.1**  $p$  y  $p^2 + 2$  son números primos si y solamente si  $p = 3$ .

**Demostración:**

(a) Supongamos que  $p$  y  $p^2 + 2$  son números primos. Para demostrar que  $p = 3$ , probemos que  $p > 1$  y  $\neg(p = 2 \vee p > 3)$ .

Por hipótesis  $p$  es primo, luego por definición de número primo  $p > 1$ .

Para la demostración de  $\neg(p = 2 \vee p > 3)$ , supongamos que  $p = 2 \vee p > 3$  y obtengamos una contradicción.

Caso  $p = 2$ . Tenemos entonces que  $p^2 + 2 = 6$  y puesto que, por el lema 6.1.3, el número  $6 = 2 \times 3$  no es primo, concluimos que  $p^2 + 2$  no es primo, lo cual contradice la hipótesis.

Caso  $p > 3$ . De aquí se tiene que  $p = 3 + k$  para algún  $k > 0$ . Ahora, por el lema 6.1.5 sabemos que  $k \bmod 3 = 0 \vee k \bmod 3 = 1 \vee k \bmod 3 = 2$ . En cualesquiera de estos

tres casos se tiene una contradicción:

Si  $k \bmod 3 = 0$  entonces 3 divide a  $k$  y por lo tanto, por el lema 6.1.6, divide a  $3 + k$ , además  $3 \neq 1$  y de  $k > 0$  tenemos que  $3 \neq 3 + k$ , por lo tanto, por el lema 6.1.3,  $3 + k$  no es primo, es decir,  $p$  no es primo, lo cual contradice la hipótesis.

Si  $k \bmod 3 = 1 \vee k \bmod 3 = 2$  entonces, por el lema 6.1.4,  $(3 + k)^2 + 2$  no es primo, es decir,  $p^2 + 2$  no es primo, lo cual contradice la hipótesis.

(b) En el otro sentido, si  $p = 3$  tenemos que, por los lemas 6.1.7 y 6.1.8,  $p$  y  $p^2 + 2 = 11$  son números primos.

□

**theorem primotres:**  $\text{prime } p \wedge \text{prime } (p^2 + 2) \longleftrightarrow p = 3$

**proof**

**assume hip:**  $\text{prime } p \wedge \text{prime } (p^2 + 2)$

**from hip have hip1:**  $\text{prime } p$  ..

**from hip have hip2:**  $\text{prime } (p^2 + 2)$  ..

**show**  $p = 3$

**proof** –

**from hip1 have**  $p > 1$  **by** (*simp add: prime-def*)

**moreover**

**have**  $\neg(p = 2 \vee p > 3)$

**proof**

**assume**  $p = 2 \vee p > 3$

**show** *False*

**proof** (*rule disjE*)

**assume**  $p = 2$

**hence**  $p^2 + 2 = 6$  **by** *simp*

**also have**  $\dots = 2 * 3$  **by** *simp*

**finally have** *ecuacion:*  $p^2 + 2 = 2 * 3$  **by** *simp*

**hence**  $2 \text{ dvd } p^2 + 2$  **by** (*simp add: dvd-def*)

**moreover**

**have**  $(2::\text{nat}) \neq 1$  **by** *simp*

**moreover**

**from** *ecuacion* **have**  $2 \neq p^2 + 2$  **by** *simp*

**ultimately have**  $\neg \text{prime } (p^2 + 2)$  **by** (*rule noprimo*)

**with hip2 show** *False* **by** *contradiction*

**next**

**assume**  $p > 3$

**hence**  $\exists k > 0. 3 + k = p$  **by** (*rule less-imp-add-positive*)

**then obtain**  $k$  **where**  $k > 0 \wedge 3 + k = p$  **by** (*rule exE*)

**from**  $k$  **have** *mayor:*  $k > 0$  ..

**from**  $k$  **have** *ecuacion:*  $3 + k = p$  ..

**have**  $k \bmod 3 = 0 \vee k \bmod 3 = 1 \vee k \bmod 3 = 2$  **by** (*rule residuotres*)

```

thus False
proof (rule disjE)
  assume  $k \bmod 3 = 0$ 
  hence  $3 \text{ dvd } k$  by (simp add: dvd-eq-mod-eq-0)
  hence  $3 \text{ dvd } (3+k)$  by (rule dividesuma)
  moreover
  have  $(3::\text{nat}) \neq 1$  by simp
  moreover
  from mayor have  $3 \neq 3+k$  by simp
  ultimately have  $\neg \text{prime}(3+k)$  by (rule noprimo)
  with ecuacion have  $\neg \text{prime } p$  by simp
  with hip1 show False by contradiction
next
  assume  $h: k \bmod 3 = 1 \vee k \bmod 3 = 2$ 
  show False
  proof –
    from  $h$  have  $\neg \text{prime}((3+k)^2+2)$  by (rule noprimoresiduo)
    with ecuacion have  $\neg \text{prime}(p^2+2)$  by simp
    with hip2 show False by contradiction
  qed
qed
qed
qed
ultimately show  $p = 3$  by simp
qed
next
  assume  $hip: p = 3$ 
  show  $\text{prime } p \wedge \text{prime } (p^2 + 2)$ 
  proof –
    from  $hip$  have  $\text{prime } p$  by (simp add: tresprimo)
    moreover
    from  $hip$  have  $\text{prime } (p^2 + 2)$  by (simp add: onceprimo)
    ultimately show ?thesis ..
  qed
qed

```

En la demostración anterior utilizamos la regla de inferencia,

$$\bullet \frac{i < j}{\exists k > 0. i + k = j} \quad (\text{less-imp-add-positive})$$

y el lema

$$\bullet (k \text{ dvd } n) = (n \bmod k = 0) \quad (\text{dvd-eq-mod-eq-0})$$

# Capítulo 7

## Números irracionales

En este capítulo ilustramos el concepto de número irracional y el uso de la operación de potenciación en los números reales para la prueba matemática, y su formalización en Isar, de la existencia de una potencia racional en términos de dos números irracionales:

*Existen  $a, b$  números irracionales tales que  $a^b$  es un número racional.*

Para la demostración de esta propiedad hemos usado las siguientes definiciones y lemas.

### 7.1 Definiciones

Un número real  $x$  es racional,  $x \in \mathbb{Q}$ , si y solamente si existen  $m, n \in \mathbb{N}$  tales que  $n \neq 0 \wedge |x| = m/n$ .

Un número real  $x$  es irracional si y solamente si  $x$  no es racional ( $x \notin \mathbb{Q}$ ).

En Isar el conjunto de los números racionales y la raíz cuadrada se definen de la siguiente manera.

#### **definition**

*rationals* :: real set (Q) **where**

$\mathbb{Q} = \{x. \exists m n. n \neq 0 \wedge |x| = \text{real } (m :: \text{nat}) / \text{real } (n :: \text{nat})\}$

#### **definition**

*root* :: nat  $\Rightarrow$  real  $\Rightarrow$  real **where**

$\text{root } n \ x \equiv (\text{SOME } u :: \text{real}. (0 < x \longrightarrow 0 < u) \wedge u^n = x)$

*sqrt* :: real  $\Rightarrow$  real **where**

$\text{sqrt } x \equiv \text{root } 2 \ x$

La potencia  $x^a$ , donde  $a, b$  son números reales con  $x > 0$ , está definida por,  $x^a = \exp(a \ln x)$ . En Isar definimos la operación de potenciación en los números reales

de la siguiente manera.

**definition**

*powr* :: [real,real] => real **where**

*x powr a = exp (a \* ln x)*

Nótese que en esta definición  $x$  puede ser cualquier número real.

## 7.2 Lemas sobre números racionales e irracionales

**Lema 7.2.1**  $2 \in \mathbb{Q}$

**Demostración:**  $|2| = 2/1$

□

**lemma** *racionaldos*:  $2 \in \mathbb{Q}$

**proof** –

**have**  $(1::nat) \neq 0 \wedge |2| = \text{real } (2::nat) / \text{real } (1::nat)$  **by** *simp*

**hence**

$\exists n. n \neq 0 \wedge |2| = \text{real } (2::nat) / \text{real } (n::nat)$  **by** *(rule exI)*

**hence**

$\exists m n. n \neq 0 \wedge |2| = \text{real } (m::nat) / \text{real } (n::nat)$  **by** *(rule exI)*

**thus** *?thesis* **by** *(simp add: rationals-def)*

**qed**

**Lema 7.2.2**  $\sqrt{2} \notin \mathbb{Q}$

**Demostración:** Puesto que 2 es un número primo se tiene que  $\sqrt{2} \notin \mathbb{Q}$ .

□

**lemma** *irracraizados*:  $\text{sqrt}(\text{real } (2::nat)) \notin \mathbb{Q}$

**proof** –

**have** *prime*  $(2::nat)$  **by** *(rule two-is-prime)*

**thus** *?thesis* **by** *(rule sqrt-prime-irrational)*

**qed**

En esta demostración hemos utilizado los lemas

- *prime* 2 *(two-is-prime)*
- *prime*  $p \implies \text{sqrt}(\text{real } p) \notin \mathbb{Q}$  *(sqrt-prime-irrational)*



## 7.3 Teorema principal

**Teorema 7.3.1** *Existen  $a, b$  números irracionales tales que  $a^b$  es un número racional.*

**Demostración:** Tenemos que  $\sqrt{2}^{\sqrt{2}}$  es un número irracional o un número racional. Mostremos que en cualesquiera de los dos casos se cumple el teorema.

Supongamos que  $\sqrt{2}^{\sqrt{2}}$  es un número irracional. Entonces, de esta hipótesis y el lema 7.2.2, tenemos que  $a = \sqrt{2}^{\sqrt{2}}$  y  $b = \sqrt{2}$  son números irracionales tales que

$$\begin{aligned} a^b &= (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} \\ &= (\sqrt{2})^{\sqrt{2}\sqrt{2}} \quad [\text{propiedad del producto de exponentes}] \\ &= (\sqrt{2})^2 \quad [\text{simplificación}] \\ &= 2 \quad [\text{simplificación}] \end{aligned}$$

Es decir, por el lema 7.2.1,  $a^b = 2$  es un número racional.

Supongamos que  $\sqrt{2}^{\sqrt{2}}$  es un número racional. Entonces, por el lema 7.2.2,  $a = b = \sqrt{2}$  son números irracionales tales que, por hipótesis,  $a^b = \sqrt{2}^{\sqrt{2}}$  es un número racional.  $\square$

**theorem racional:**  $\exists a b. a \notin \mathbb{Q} \wedge b \notin \mathbb{Q} \wedge a \text{ powr } b \in \mathbb{Q}$

**proof** –

let  $?q = \text{sqrt}(\text{real } (2::\text{nat}))$

let  $?p = ?q \text{ powr } ?q$

have  $?p \notin \mathbb{Q} \vee ?p \in \mathbb{Q}$  by (rule excluded-middle)

thus ?thesis

**proof cases**

assume  $?p \in \mathbb{Q}$

with irracraizados have

$?q \notin \mathbb{Q} \wedge ?q \notin \mathbb{Q} \wedge ?q \text{ powr } ?q \in \mathbb{Q}$  by simp

hence

$\exists b. ?q \notin \mathbb{Q} \wedge b \notin \mathbb{Q} \wedge ?q \text{ powr } b \in \mathbb{Q}$  by (rule exI)

thus

$\exists a b. a \notin \mathbb{Q} \wedge b \notin \mathbb{Q} \wedge a \text{ powr } b \in \mathbb{Q}$  by (rule exI)

next

assume  $?p \notin \mathbb{Q}$

moreover

have  $?p \text{ powr } ?q \in \mathbb{Q}$

**proof** –

have  $?q > 0$  by simp

hence simplif:  $\text{real } (2::\text{nat}) * \ln ?q = \ln (?q^2)$  by (rule sym[OF ln-realpow])

have  $?p \text{ powr } ?q = ?q \text{ powr } (?q * ?q)$  by (simp only: powr-powr)

```

also have ... = ?q powr ?q^2 by (simp only: power2-eq-square)
also have ... = ?q powr 2 by (simp add: real-sqrt-pow2-iff)
also have ... = exp(real (2::nat) * ln ?q) by(simp add: powr-def)
also have ... = exp(ln (?q^2)) by(simp only: simplif)
also have ... = ?q^2 by simp
also have ... = 2 by (simp add: real-sqrt-pow2-iff)
also have ... ∈ ℚ by (rule racionaldos)
finally show ?p powr ?q ∈ ℚ by simp
qed
moreover
have ?q ∉ ℚ by (rule irracraizados)
ultimately have
?p ∉ ℚ ∧ ?q ∉ ℚ ∧ ?p powr ?q ∈ ℚ by simp
hence
∃ b. ?p ∉ ℚ ∧ b ∉ ℚ ∧ ?p powr b ∈ ℚ by (rule exI)
thus
∃ a b. a ∉ ℚ ∧ b ∉ ℚ ∧ a powr b ∈ ℚ by (rule exI)
qed
qed

```

En la demostración anterior hemos utilizado los lemas

- $0 < x \implies \ln (x ^ n) = \text{real } n * \ln x$  (ln-realpow)
- $(x \text{ powr } a) \text{ powr } b = x \text{ powr } (a * b)$  (powr-powr)
- $((\text{sqrt } x)^2 = x) = (0 \leq x)$  (real-sqrt-pow2-iff)

# Capítulo 8

## Completitud de los números reales

En este capítulo utilizamos la propiedad de completitud de los números reales para demostrar el siguiente teorema.

**Teorema 8.0.2** Consideremos  $(A, +, -)$  un conjunto no vacío junto con dos operaciones binarias  $+, -$ , y  $f, g$  dos funciones de  $A$  en  $\mathbb{R}$ . Supongamos que:

1. para todo  $x, y$ ,  $f(x + y) + f(x - y) = 2f(x)g(y)$
2.  $f$  no es la función cero
3.  $|f(x)| \leq 1$  para todo  $x$ .

Entonces  $|g(x)| \leq 1$  para todo  $x$ .

Una demostración informal del teorema anterior es la siguiente.

**Demostración:** Sea  $k$  el supremo del conjunto  $B = \{|f(x)| \mid x \in A\}$ . Supongamos que  $|g(y)| > 1$ . Entonces

$$2k \geq |f(x + y)| + |f(x - y)| \geq |f(x + y) + f(x - y)| = 2|g(y)||f(x)|,$$

por lo tanto  $|f(x)| \leq k/|g(y)|$ . Es decir,  $k/|g(y)|$  es una cota superior de  $B$  menor que  $k$ . Contradicción. □

Para la formalización de esta demostración en Isar, en la sección que sigue precisamos los conceptos de cota superior, elemento mínimo y supremo, junto con las correspondientes definiciones en Isar, y establecemos como lemas los hechos implícitos usados en la argumentación anterior.

## 8.1 Algunos conceptos y lemas sobre números reales

Sea  $(R, \leq)$  un conjunto parcialmente ordenado y  $S \subseteq R$ .

**Definición 8.1.1 (Cota superior)**  $x$  es una cota superior de  $S$  si y solamente si  $\forall y \in S. y \leq x$ .

En Isar se utiliza la notación  $S * \leq x$ , para indicar que  $x$  es una cota superior de  $S$ .

**definition**

```
setle      :: ['a set, 'a::ord] => bool  ( infixl * \leq 70) where
S * \leq x = ( $\forall y \in S. y \leq x$ )
```

**Definición 8.1.2**  $x$  es una cota superior de  $S$  en  $R$  si y solamente si  $x$  es una cota superior de  $S$  y  $x \in R$ .

En Isar se utiliza la notación  $isUb R S x$ , para indicar que  $x$  es una cota superior de  $S$  en  $R$ .

**definition**

```
isUb      :: ['a set, 'a set, 'a::ord] => bool where
isUb R S x = (S * \leq x  $\wedge$   $x \in R$ )
```

**Definición 8.1.3 (Cota inferior)**  $x$  es una cota inferior de  $S$  si y solamente si  $\forall y \in S. x \leq y$ .

En Isar se utiliza la notación  $x \leq * S$ , para indicar que  $x$  es una cota inferior de  $S$ .

**definition**

```
setge     :: ['a::ord, 'a set] => bool  ( infixl <=* 70) where
x <=* S = ( $\forall y \in S. x \leq y$ )
```

**Definición 8.1.4 (Elemento mínimo)**  $x$  es el elemento mínimo de  $R$  si y solamente si  $x \in R$  y  $x$  es una cota inferior de  $R$ .

En Isar se utiliza la notación  $leastP R x$  para indicar que  $x$  es el mínimo de  $R$ .

**definition**

```
leastP    :: ['a => bool, 'a::ord] => bool where
leastP P x = (P x  $\wedge$  x <=* Collect P)
```

**Definición 8.1.5 (Supremo)** Sea  $CS(R, S) = \{x \in R \mid x \text{ es una cota superior de } S\}$  el conjunto parcialmente ordenado de cotas superiores de  $S$ , con el orden inducido por  $R$ .  $x$  es el supremo de  $S$  con respecto a  $R$  si y solamente si  $x$  es el elemento mínimo de  $CS(R, S)$ .

En matemáticas para indicar que  $x$  es el supremo de  $S$  con respecto a  $R$  escribimos  $a = \sup_R S$ , y en Isar se escribe  $isLub R S x$ .

**definition**

$isLub \quad :: [ 'a \text{ set}, 'a \text{ set}, 'a::ord ] \Rightarrow bool$  **where**

$isLub R S x = leastP (isUb R S) x$

Se dice que el conjunto  $S$  está acotado superiormente si tiene al menos una cota superior.

Consideremos el conjunto de números reales  $\mathbb{R}$  con el orden natural  $\leq$ . Entonces tenemos la siguiente propiedad.

**Lema 8.1.6 (Completitud de los números reales)** *Todo conjunto  $S$  no vacío de números reales acotado superiormente tiene supremo.*

En Isar se enuncia esta propiedad de la siguiente forma.

**lemma** *reals-complete:*

*assumes* *notempty-S*:  $\exists X. X \in S$

*and exists-Ub*:  $\exists Y. isUb (UNIV::real \text{ set}) S Y$

*shows*  $\exists t. isLub (UNIV :: real \text{ set}) S t$

**Lema 8.1.7** *Sea  $f$  una función de valores reales. Supongamos que  $|f(x)| \leq 1$  para todo  $x$ . Entonces existe  $k$  tal que  $k = \sup_{\mathbb{R}} \{z \mid \exists x. |f(x)| = z\}$ .*

**Demostración:** Sea  $a$  un elemento del dominio de  $f$ , entonces  $z = |f(a)| \in \{z \mid \exists x. |f(x)| = z\}$ . Luego  $\{z \mid \exists x. |f(x)| = z\} \neq \emptyset$ , además, por hipótesis, 1 es una cota superior de  $\{z \mid \exists x. |f(x)| = z\}$ . Por lo tanto, por la propiedad de *completitud de los números reales*, existe  $k$  tal que  $k = \sup_{\mathbb{R}} \{z \mid \exists x. |f(x)| = z\}$ . □

**lemma** *existe-sup*: **fixes**  $f:: 'a \Rightarrow real$

**assumes** *hip*:  $\forall x. |f(x)| \leq 1$

**shows**  $\exists k. isLub UNIV \{z. \exists x. |f(x)| = z\} k$

**proof** (*rule reals-complete*)

**show**  $\exists X. X \in \{z. \exists x. |f(x)| = z\}$  **by** *auto*

**next**

**show**  $\exists Y. \text{isUb UNIV } \{z. \exists x. |f(x)| = z\} Y$

**proof** –

**from hip** have  $\forall y \in \{z. \exists x. |f(x)| = z\}. y \leq 1$  **by auto**

**hence**  $\{z. \exists x. |f(x)| = z\} * \leq 1$  **by (rule settleI)**

**moreover**

**have**  $1 \in \text{UNIV}$  **by auto**

**ultimately have**  $\text{isUb UNIV } \{z. \exists x. |f(x)| = z\} 1$  **by (rule isUbI)**

**thus**  $\exists Y. \text{isUb UNIV } \{z. \exists x. |f(x)| = z\} Y$  **by (rule exI)**

**qed**

**qed**

En la demostración anterior hemos utilizado las reglas de inferencia,

$$\bullet \frac{\forall y \in S. y \leq x}{S * \leq x} \quad (\text{settleI})$$

$$\bullet \frac{S * \leq x \quad x \in R}{\text{isUb } R \ S \ x} \quad (\text{isUbI})$$

**Lema 8.1.8** *Sea  $f$  una función de valores reales. Supongamos que  $f(x) \neq 0$  para algún  $x$  y  $k = \sup_{\mathbb{R}} \{z \mid \exists x. |f(x)| = z\}$ , entonces  $|f(x)| \leq k$  para todo  $x$  y  $k > 0$ .*

**Demostración:** Sea  $a$  un elemento cualquiera del dominio de  $f$ , entonces  $z = |f(a)| \in \{z \mid \exists x. |f(x)| = z\}$  y por consiguiente  $|f(a)| \leq k$ , ya que por hipótesis  $k$  es una cota superior de  $\{z \mid \exists x. |f(x)| = z\}$ . También, por hipótesis, existe  $x$  tal que  $f(x) \neq 0$ , luego  $0 < |f(x)|$ , y puesto que  $|f(x)| \leq k$ , entonces  $k > 0$ .

□

**lemma propiedad-sup:** **fixes**  $f:: 'a \Rightarrow \text{real}$

**assumes** *hip1:*  $\exists x. f(x) \neq 0$

**and** *hip2:*  $\text{isLub UNIV } \{z. \exists x. |f(x)| = z\} k$

**shows**  $\forall x. |f(x)| \leq k \wedge k > 0$

**proof** –

**have**  $a: \forall x. |f(x)| \leq k$

**proof**

**fix**  $x$

**show**  $|f(x)| \leq k$

**proof** –

**have**  $|f(x)| \in \{z. \exists x. |f(x)| = z\}$  **by auto**

**with** *hip2* **show**  $|f(x)| \leq k$  **by (rule isLubD2)**

**qed**

**qed**

moreover

have  $k > 0$

proof –

from *hip1* obtain  $w$  where  $f w \neq 0$  ..

then have  $|f(w)| > 0$  by *arith*

also have  $k \geq |f(w)|$  using *a* by *auto*

finally show  $k > 0$  by *arith*

qed

ultimately show *?thesis* by *auto*

qed

En la demostración anterior utilizamos la regla de inferencia,

$$\bullet \frac{\text{isLub } R \ S \ x \quad y \in S}{y \leq x} \quad (\text{isLubD2})$$

**Lema 8.1.9** Sea  $(A, +, -)$  un conjunto no vacío junto con dos operaciones binarias  $+, -$ ,  $f : A \rightarrow \mathbb{R}$ , y  $g$  una función de valores reales. Supongamos que para todo  $x, y$ ,  $f(x + y) + f(x - y) = 2f(x)g(y)$  y  $|f(x)| \leq k$ . Entonces, para todo  $x, y$  tal que  $x \in A$  y  $y$  pertenece al dominio de  $g$ ,  $|g(y)||f(x)| \leq k$ .

**Demostración:**

$$\begin{aligned} 2|g(y)||f(x)| &= |f(x + y) + f(x - y)| && \text{[por hipótesis]} \\ &\leq |f(x + y)| + |f(x - y)| && \text{[por desigualdad del triángulo]} \\ &\leq 2k && \text{[por hipótesis]} \end{aligned}$$

Por lo tanto,  $|g(y)||f(x)| \leq k$ .

□

**lemma producto-funciones:** **fixes**  $f :: 'a :: \{\text{plus, minus}\} \Rightarrow \text{real}$

**fixes**  $g :: 'a \Rightarrow \text{real}$

**assumes** *hip1*:  $\forall x y. f(x + y) + f(x - y) = 2 * f x * g y$

**and** *hip2*:  $\forall x. |f(x)| \leq k$

**shows**  $\forall y x. |g(y)| * |f(x)| \leq k$

**proof**

**fix**  $y$

**show**  $\forall x. |g(y)| * |f(x)| \leq k$

**proof**

**fix**  $x$

**show**  $|g(y)| * |f(x)| \leq k$

**proof** –

**have**  $2 * |g(y)| * |f(x)| = |f(x + y) + f(x - y)|$

```

    using hip1 by(auto simp add: abs-mult)
  also have ... ≤ |f(x + y)| + |f(x - y)|
    by (rule abs-triangle-ineq)
  also have ... ≤ 2 * k
  proof -
    from hip2 have |f(x+y)| ≤ k by (rule-tac x=x+y in allE)
    moreover
    from hip2 have |f(x-y)| ≤ k by (rule-tac x=x-y in allE)
    ultimately show ?thesis by arith
  qed
  finally have (2*|g(y)|) * |f(x)| ≤ 2 * k .
  thus ?thesis by (simp add: mult-commute)
qed
qed
qed

```

En la prueba anterior utilizamos los lemas,

- $|a * b| = |a| * |b|$  (abs-mult)
- $|a + b| ≤ |a| + |b|$  (abs-triangle-ineq)

**Lema 8.1.10** Sean  $f, g$  funciones de valores reales. Supongamos que  $1 < |g(y)|$  y para todo  $x$ ,  $|g(y)||f(x)| ≤ k$ . Entonces,  $k/|g(y)|$  es una cota superior de  $\{z \mid \exists x. |f(x)| = z\}$ .

**Demostración:** Sea  $z \in \{z \mid \exists x. |f(x)| = z\}$ , entonces existe  $x$  tal que  $z = |f(x)|$ , luego, por hipótesis,  $|g(y)|z = |g(y)||f(x)| ≤ k$  y puesto que, por hipótesis,  $|g(y)| > 0$ , tenemos que  $z ≤ k/|g(y)|$ , y por lo tanto  $k/|g(y)|$  es una cota superior de  $\{z \mid \exists x. |f(x)| = z\}$ . □

```

lemma cota-superior: fixes f:: 'a ⇒ real
  fixes g:: 'a ⇒ real
  assumes hip1: 1 < |g(y)|
  and hip2: ∀ x. |g(y)| * |f(x)| ≤ k
  shows isUb UNIV {z. ∃ x. |f(x)| = z} (k / |g(y)|)
proof -
  have ∀ x. |f(x)| ≤ k / |g(y)|
  proof
    fix x
    show |f(x)| ≤ k / |g(y)|

```



**proof** –

**from** *hip1* **have**  $0 < |g(y)|$  **by** *arith*

**hence**

$(|f(x)| \leq k / |g(y)|) = (|f(x)| * |g(y)| \leq k)$

**by** (*rule pos-le-divide-eq*)

**moreover**

**from** *hip2* **have**  $|g(y)| * |f(x)| \leq k$  **by** (*rule allE*)

**hence**  $|f(x)| * |g(y)| \leq k$  **by** (*simp add: mult-commute*)

**ultimately show** *?thesis* **by** *simp*

**qed**

**qed**

**hence**  $\forall Y \in \{z. \exists x. |f(x)| = z\}. Y \leq (k / |g(y)|)$  **by** *auto*

**hence**  $\{z. \exists x. |f(x)| = z\} * \leq (k / |g(y)|)$  **by** (*rule setleI*)

**moreover**

**have**  $k / |g(y)| \in UNIV$  **by** *auto*

**ultimately show** *isUbl UNIV*  $\{z. \exists x. |f(x)| = z\} (k / |g(y)|)$

**by** (*rule isUbl*)

**qed**

En la prueba anterior utilizamos el lema

- $(0 < 'a) < c \implies (a \leq b / c) = (a * c \leq b)$  (*pos-le-divide-eq*)

**Lema 8.1.11** Sea  $u = \sup_{\mathbb{R}} S$ . Si  $x < u$  entonces  $x$  no es una cota superior de  $S$ .

**Demostración:** Si  $x$  es una cota superior, entonces, por definición de supremo,  $u \leq x$ . Luego, por hipótesis,  $x < u \leq x$ . Así obtenemos la contradicción  $x < x$ . □

**lemma** *menor-supremo-no-cota*: **fixes**  $x::'a::order$

**assumes** *hip1*: *isLub U S u* **and** *hip2*:  $x < u$

**shows**  $\neg isUbl U S x$

**proof**

**assume** *hipaux*: *isUbl U S x*

**from** *hip1* **have**  $u \leq x$  **by** (*rule isLub-le-isUbl*)

**with** *hip2* **show** *False* **by** *auto* — *rule less-le-trans*

**qed**

**Lema 8.1.12** Sean  $f, g$  funciones de valores reales. Supongamos que  $1 < |g(y)|$ ,  $k = \sup_{\mathbb{R}} \{z \mid \exists x. |f(x)| = z\}$  y  $k > 0$ . Entonces  $k / |g(y)|$  no es cota superior de  $\{z \mid \exists x. |f(x)| = z\}$ .

**Demostración:** De las hipótesis  $1 < |g(y)|$  y  $k > 0$ , tenemos que  $k < k|g(y)|$  y por lo tanto,  $k/|g(y)| < k$ . Entonces, por el lema 8.1.11,  $k/|g(y)|$  no es cota superior de  $\{z \mid \exists x. |f(x)| = z\}$ .

□

En la demostración anterior utilizamos la regla de inferencia,

$$\bullet \frac{\text{isLub } R \ S \ x \quad \text{isUb } R \ S \ y}{x \leq y} \quad (\text{isLub-le-isUb})$$

**lemma no-cota-superior:** *fixes*  $f :: 'a \Rightarrow \text{real}$

*fixes*  $g :: 'a \Rightarrow \text{real}$

*assumes*  $\text{hip1}: 1 < |g(y)|$

*and*  $\text{hip2}: \text{isLub } \text{UNIV } \{z. \exists x. |f(x)| = z\} \ k$

*and*  $\text{hip3}: k > 0$

*shows*

$\neg \text{isUb } \text{UNIV } \{z. \exists x. |f(x)| = z\} (k / |g(y)|)$

**proof** –

**have**  $k / |g(y)| < k$

**proof** –

**from**  $\text{hip1}$  **have**  $0 < |g(y)|$  **by** *arith*

**moreover**

**from**  $\text{hip3}$  **and**  $\text{hip1}$  **have**  $k * 1 < k * |g(y)|$  **by** (*rule real-mult-less-mono2*)

**hence**  $k < k * |g(y)|$  **by** *arith*

**ultimately show** *?thesis* **by** (*rule mult-imp-div-pos-less*)

**qed**

**with**  $\text{hip2}$  **show** *?thesis* **by** (*rule menor-supremo-no-cota*)

**qed**

En la demostración anterior hemos utilizado las reglas de inferencia,

$$\bullet \frac{0 < z \quad x < y}{z * x < z * y} \quad (\text{real-mult-less-mono2})$$

$$\bullet \frac{(0 :: 'a) < y \quad x < z * y}{x / y < z} \quad (\text{mult-imp-div-pos-less})$$

## 8.2 Demostración del teorema principal

**Teorema 8.2.1 (función acotada)** *Consideremos*  $(A, +, -)$  *un conjunto no vacío junto con dos operaciones binarias*  $+, -$ , *y*  $f, g$  *dos funciones de*  $A$  *en*  $\mathbb{R}$ . *Supongamos que:*

1. para todo  $x, y$ ,  $f(x + y) + f(x - y) = 2f(x)g(y)$
2.  $f$  no es la función cero
3.  $|f(x)| \leq 1$  para todo  $x$ .

Entonces  $|g(x)| \leq 1$  para todo  $x$ .

**Demostración:** (por contradicción). Supongamos (d)  $1 < |g(x)|$  para algún  $x$ .

De la hipótesis (c) tenemos que, por el lema 8.1.7, existe  $k$  tal que (i)  $k = \sup_{\mathbb{R}} \{z \mid \exists x. |f(x)| = z\}$ . De esto último y la hipótesis (b) tenemos por el lema 8.1.8, (ii)  $|f(x)| \leq k$  y (iii)  $k > 0$ . De (ii) y la hipótesis (a) tenemos que, por el lema 8.1.9, para todo  $x$ ,  $|g(y)||f(x)| \leq k$ . De esto último y la hipótesis (d) tenemos, por el lema 8.1.10, (iv)  $k/|g(y)|$  es una cota superior de  $\{z \mid \exists x. |f(x)| = z\}$ .

Por otro lado, de (iii), (d) y (i) tenemos, por el lema 8.1.12, (v)  $k/|g(y)|$  no es cota superior de  $\{z \mid \exists x. |f(x)| = z\}$ . De esta forma, de (iv) y (v), obtenemos una contradicción. Por lo tanto,  $|g(x)| \leq 1$  para todo  $x$ .

□

**theorem** *funcion-acotada*: **fixes**  $f:: 'a::\{plus, minus\} \Rightarrow real$

**fixes**  $g:: 'a \Rightarrow real$

**assumes** *hip1*:  $\forall x y. f(x + y) + f(x - y) = 2 * f x * g y$

**and** *hip2*:  $\exists x. f(x) \neq 0$

**and** *hip3*:  $\forall x. |f(x)| \leq 1$

**shows**  $\forall y. |g(y)| \leq 1$

**proof**

**fix**  $y$

**have**  $\neg |g(y)| > 1$

**proof**

**assume** *hip-aux*:  $1 < |g(y)|$

**from** *hip3* **have**  $\exists k. isLub UNIV \{z. \exists x. |f(x)| = z\} k$

**by** (*rule existe-sup*)

**then obtain**  $k$  **where**  $b: isLub UNIV \{z. \exists x. |f(x)| = z\} k$  **by** *auto*

**with** *hip2* **have**  $h: \forall x. |f(x)| \leq k \wedge k > 0$  **by** (*rule propiedad-sup*)

**hence**  $\forall x. |f(x)| \leq k$  **by** *auto*

**with** *hip1* **have**  $\forall y x. |g(y)| * |f(x)| \leq k$

**by** (*rule producto-funciones*)

**hence**  $\forall x. |g(y)| * |f(x)| \leq k$  **by** (*rule allE*)

**with** *hip-aux* **have**  $isUb UNIV \{z. \exists x. |f(x)| = z\} (k / |g(y)|)$

**by** (*rule cota-superior*)

**moreover**

**from**  $h$  **have**  $k > 0$  **by** *auto*

**with** *hip-aux* **and**  $b$  **have**  $\neg isUb UNIV \{z. \exists x. |f(x)| = z\} (k / |g(y)|)$

**by** (*rule no-cota-superior*)

**ultimately show** *False by auto*  
**qed**  
**thus**  $|g(y)| \leq 1$  *by auto*  
**qed**

Como corolario, tenemos el caso especial en que  $f, g$  son funciones reales con valores reales.

**Corolario 8.2.2** Sean  $f, g : \mathbb{R} \rightarrow \mathbb{R}$ . Supongamos que:

1. para todo  $x, y$ ,  $f(x + y) + f(x - y) = 2f(x)g(y)$
2.  $f$  no es la función cero
3.  $|f(x)| \leq 1$  para todo  $x$ .

Entonces  $|g(x)| \leq 1$  para todo  $x$ .

**Demostración:** Basta con aplicar el teorema anterior. □

**theorem** *fixes f:: real ⇒ real*  
**fixes** *g:: real ⇒ real*  
**assumes** *hip1: ∀ x y. f(x + y) + f(x - y) = 2 \* f x \* g y*  
**and** *hip2: ∃ x. f(x) ≠ 0*  
**and** *hip3: ∀ x. |f(x)| ≤ 1*  
**shows** *∀ y. |g(y)| ≤ 1*  
**proof** –  
**show** *?thesis* **by**(*rule funcion-acotada*)  
**qed**

# Capítulo 9

## Geometría proyectiva

En el libro de Heyting [3, cap 2] se presenta de manera axiomática las principales propiedades del plano proyectivo; se introducen las nociones de punto y recta (estructuras) y el de relación de incidencia como entidades geométricas primitivas. Posteriormente, a partir de un número determinado de axiomas y algunas definiciones básicas, se caracterizan las relaciones existentes entre estas entidades primitivas.

El objetivo de este capítulo es formalizar en Isar parte de este estudio axiomático de la geometría proyectiva y verificar mecánicamente algunas de las propiedades enunciadas en el texto de Heyting. En particular, probar en Isar la proposición generalizada de Desargues.

### 9.1 Declaración de tipos para la geometría proyectiva

Para describir en Isar los axiomas de la geometría proyectiva declaramos como tipos los objetos primitivos punto y recta:

```
typedecl punto
typedecl recta
```

Obsérvese que estos tipos no están definidos, de modo que nada acerca de ellos es conocido excepto que son no vacíos.

También declaramos una relación de incidencia:

```
consts
  incidente :: punto  $\Rightarrow$  recta  $\Rightarrow$  bool
```

Este predicado de dos argumentos representa la noción de “pertenencia” de un punto a una recta. Para referirnos a *incidente P l* decimos que, “el punto *P* es incidente con la recta *l*” o “la recta *l* es incidente con el punto *P*”. Los siguientes lemas ilustran los anteriores conceptos.

**Lema 9.1.1** *Si el punto  $p$  es incidente con la recta  $l_1$  pero no con la recta  $l_2$ , entonces las rectas  $l_1$  y  $l_2$  son distintas.*

**lemma** *lineas-distintas:*

**assumes** *incidente p l1*

**and** *¬incidente p l2*

**shows**  $l1 \neq l2$

**proof**

**assume**  $l1=l2$

**with** *assms* **have** *incidente p l1*  $\wedge$  *¬incidente p l1* **by** *simp*

**thus** *False* **by** *simp*

**qed**

**Lema 9.1.2** *Si el punto  $p_1$  es incidente con la recta  $l$  y el punto  $p_2$  no lo es, entonces los puntos  $p_1$  y  $p_2$  son distintos.*

**lemma** *puntos-distintos:*

**assumes** *incidente p1 l*

**and** *¬incidente p2 l*

**shows**  $p1 \neq p2$

**proof**

**assume**  $p1=p2$

**with** *assms* **have** *incidente p1 l*  $\wedge$  *¬incidente p1 l* **by** *simp*

**thus** *False* **by** *simp*

**qed**

Usando el comando *metis*, tenemos la demostración automática de estos lemas.

**lemma** *lineas-distintas-autom: incidente p l1*  $\wedge$  *¬incidente p l2*  $\longrightarrow$   $l1 \neq l2$

**by** *metis*

**lemma** *puntos-distintos-autom:*

*incidente p1 l*  $\wedge$  *¬incidente p2 l*  $\longrightarrow$   $p1 \neq p2$

**by** *metis*

## 9.2 Los axiomas de la geometría proyectiva

En la sección 2.1 del libro de Heyting se consideran los siguientes cuatro axiomas para la geometría proyectiva.

V1a: Dados dos puntos diferentes, existe por lo menos una recta que los contiene.

V1b: Dados dos puntos diferentes, existe a lo más una recta que los contiene.

V2: Dadas dos rectas diferentes, existe por lo menos un punto que está en ambas rectas.

V3: Existen por lo menos cuatro puntos tales que ninguna recta contine cada tres de ellos.

Sin embargo, como se demostrará más adelante, el axioma (V3) puede ser reemplazado por los siguientes dos axiomas:

V4: Cada recta contiene por lo menos tres puntos distintos.

V5: No todos los puntos pertenecen a la misma recta.

En esta sección formalizamos en Isar el sistema de axiomas (V1a), (V1b), (V2), (V4) y (V5) para la geometría proyectiva.

#### axioms

*axiomv1a*:  $p1 \neq p2 \longrightarrow (\exists l. \text{incidente } p1 \ l \wedge \text{incidente } p2 \ l)$

*axiomv1b*:  $p1 \neq p2 \wedge (\text{incidente } p1 \ l1 \wedge \text{incidente } p2 \ l1) \wedge (\text{incidente } p1 \ l2 \wedge \text{incidente } p2 \ l) \longrightarrow l1=l2$

*axiomv2*:  $l1 \neq l2 \longrightarrow (\exists p. \text{incidente } p \ l1 \wedge \text{incidente } p \ l2)$

*axiomv4*:  $\exists p1 \ p2 \ p3. p1 \neq p2 \wedge p1 \neq p3 \wedge p2 \neq p3 \wedge \text{incidente } p1 \ l \wedge \text{incidente } p2 \ l \wedge \text{incidente } p3 \ l$

*axiomv5*:  $\exists p. \neg \text{incidente } p \ l$

Por ejemplo, el siguiente lema se obtiene aplicando el *axiomv1b*

**Lema 9.2.1** *Dos puntos distintos son incidentes a lo sumo con una recta.*

**lemma** *lineas-iguales*:

**assumes**  $p \neq q$

**and** *incidente*  $p \ l1$

**and** *incidente*  $q \ l1$

**and** *incidente*  $p \ l2$

**and** *incidente*  $q \ l2$

**shows**  $l1 = l2$

**proof** –

**have**  $p \neq q \wedge (\text{incidente } p \ l1 \wedge \text{incidente } q \ l1) \wedge (\text{incidente } p \ l2 \wedge \text{incidente } q \ l2)$

**using** *assms* **by** *simp*

**thus** *thesis* **by** (*rule mp*[OF *axiomv1b*])

**qed**

### 9.3 Consecuencias básicas de los axiomas

Usando los anteriores axiomas demostraremos algunas propiedades del plano proyectivo; ilustraremos como, en general, en contraste con la demostración matemática, la prueba mecánica requiere considerar explícitamente los diferentes casos de incidencia entre puntos y rectas.

El axioma (V1a) afirma la existencia de una recta que pasa por dos puntos distintos y el axioma (V1b) garantiza su unicidad. Correspondiente al axioma (V1a), el axioma (V2) asegura la existencia de un punto que está en dos rectas distintas, sin embargo, la proposición sobre la unicidad del punto, correspondiente al axioma (V1b), no es considerada como un axioma ya que puede derivarse de (V1a), (V1b), (V2). Más precisamente, en el siguiente teorema demostramos que solo es necesario el axioma (V1b) para su demostración.

**Teorema 9.3.1** *Dados dos rectas diferentes, existe a lo más un punto incidente con las dos rectas.*

La demostración automática del teorema es

**theorem** DV1b-autom:

$$l1 \neq l2 \wedge$$

$$(incidente\ p1\ l1 \wedge incidente\ p2\ l1) \wedge$$

$$(incidente\ p1\ l2 \wedge incidente\ p2\ l2)$$

$$\longrightarrow p1=p2$$

**by** (metis axiomv1b)

La demostración estructurada es

**theorem** DV1b:

**assumes**  $l1 \neq l2$

**and** *incidente*  $p1\ l1$

**and** *incidente*  $p2\ l1$

**and** *incidente*  $p1\ l2$

**and** *incidente*  $p2\ l2$

**shows**  $p1 = p2$

**proof** (rule ccontr)

**assume**  $p1 \neq p2$  **show** False

**proof** –

**have**  $p1 \neq p2 \wedge (incidente\ p1\ l1 \wedge incidente\ p2\ l1) \wedge (incidente\ p1\ l2 \wedge incidente\ p2\ l2)$

**using** *assms* **by** *simp*

**hence**  $l1=l2$  **by** (rule mp[OF axiomv1b])

**moreover** **have**  $l1 \neq l2$  **using** *assms* **by** *simp*

**ultimately** **show** False **by** *simp*

**qed**



qed

Si intercambiamos “punto” y “recta” en los axiomas (V4) y (V5) obtenemos respectivamente los siguientes dos teoremas (DV4) y (DV5).

**Teorema 9.3.2 (DV4)** *Cada punto está contenido en por lo menos tres rectas distintas.*

**Demostración:** Sea  $p$  un punto cualquiera. Por el principio del tercero excluido se tiene que para cualquier recta  $l_1$ ,  $p$  es incidente con  $l_1$  o  $p$  no es incidente con  $l_1$ . De lo anterior, demostramos por casos el teorema.

1) Supongamos que  $p$  es incidente con  $l_1$ . Por el axioma (V5), existe un punto  $p_1$  que no es incidente con  $l_1$ . Por lo tanto  $p \neq p_1$ ; luego, por el axioma (V1a), existe una recta  $l_2$  tal que  $p$  y  $p_1$  son incidentes con  $l_2$ . De lo anterior tenemos que  $p_1$  es incidente con  $l_2$  y no es incidente con  $l_1$ , luego  $l_1 \neq l_2$ . De la misma forma, por el axioma (V5), existe un punto  $p_a$  que no es incidente con  $l_2$ . Por lo tanto  $p_a \neq p_1$ ; luego, por el axioma (V1a), existe una recta  $l_{aux}$  tal que  $p_a$  y  $p_1$  son incidentes con  $l_{aux}$ . De lo anterior tenemos que  $p_a$  es incidente con  $l_{aux}$  y no es incidente con  $l_2$ , luego  $l_{aux} \neq l_2$ . Además, puesto que  $p_1$  es incidente con  $l_{aux}$  y no es incidente con  $l_1$  tenemos que  $l_{aux} \neq l_1$ .

Ahora, mostramos la existencia de un punto  $p_2 \neq p_1$  que es incidente con  $l_{aux}$  pero no es incidente con  $l_1$  (ver Figura 9.1).

Por el principio del tercero excluido se tiene que,  $p_a$  es incidente con  $l_1$  o  $p_a$  no es incidente con  $l_1$ . De lo anterior, demostramos por casos la existencia de  $p_2$ .

a) Supongamos que  $p_a$  es incidente con  $l_1$ . Por el axioma (V4) existen tres puntos distintos incidentes con  $l_{aux}$  y puesto que  $p_1$  y  $p_a$  son puntos distintos e incidentes con  $l_{aux}$ , se concluye que existe  $p_2$  distinto de  $p_1$  y  $p_a$  e incidente con  $l_{aux}$ . Ahora,  $p_2$  no es incidente con  $l_1$  ya que en el caso contrario, usando  $p_2 \neq p_a$ ,  $p_a$  incidente con  $l_1$ , y  $p_2, p_a$  incidentes con  $l_1$ , tenemos por el axioma (V1b) que  $l_1 = l_{aux}$ , lo cual es falso.

b) Supongamos que  $p_a$  no es incidente con  $l_1$ . Puesto que  $p_a \neq p_1$  y es incidente con  $l_{aux}$ , entonces existe  $p_2 = p_a$  con las propiedades requeridas.

Ahora, mostramos la existencia de una recta  $l_3$  tal que  $p$  es incidente con  $l_3$ ,  $l_3 \neq l_1$  y  $l_3 \neq l_2$ .

Puesto que  $p$  es incidente con  $l_1$  y  $p_2$  no es incidente con  $l_1$ , tenemos que  $p \neq p_2$ . De aquí, por el axioma (V1a), existe una recta  $l_3$  tal que  $p$  y  $p_2$  son incidentes con  $l_3$ . Además, como  $p_2$  no es incidente con  $l_1$ , se tiene que  $l_3 \neq l_1$ .

Tenemos también que  $p_2$  no es incidente con  $l_2$ , ya que en el caso contrario, usando  $p_2 \neq p_1$ ,  $p_1$  incidente con  $l_2$ , y  $p_1, p_2$  incidentes con  $l_{aux}$ , tenemos por el axioma (V1b) que  $l_2 = l_{aux}$ , lo cual es falso. Por otro lado  $p_2$  es incidente con  $l_3$ , luego  $l_3 \neq l_2$ .

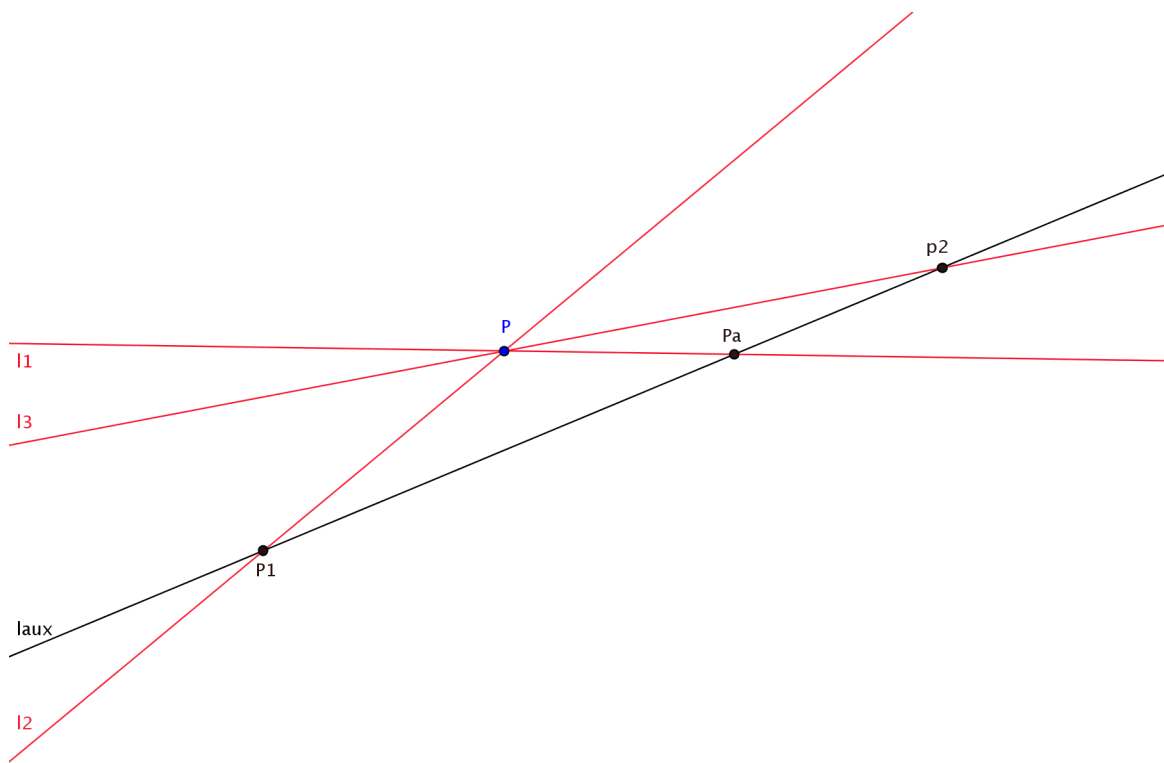


Figura 9.1: Teorema 9.3.2 (DV4)

En total, suponiendo que  $p$  es incidente con  $l_1$ , hemos demostrado la existencia de tres rectas distintas  $l_1, l_2, l_3$  que contienen al punto  $p$ .

2) Supongamos que  $p$  no es incidente con  $l_1$ . Por el axioma (V4), existen tres puntos distintos  $p_1, p_2, p_3$  incidentes con  $l_1$ . Luego  $p, p_1, p_2, p_3$  son distintos. Por lo tanto, por el axioma (V1a), existe  $l$  tal que  $p, p_1$  son incidentes con  $l$ , existe  $l_2$  tal que  $p, p_2$  son incidentes con  $l_2$ , y existe  $l_3$  tal que  $p, p_3$  son incidentes con  $l_3$  (ver Figura 9.2).

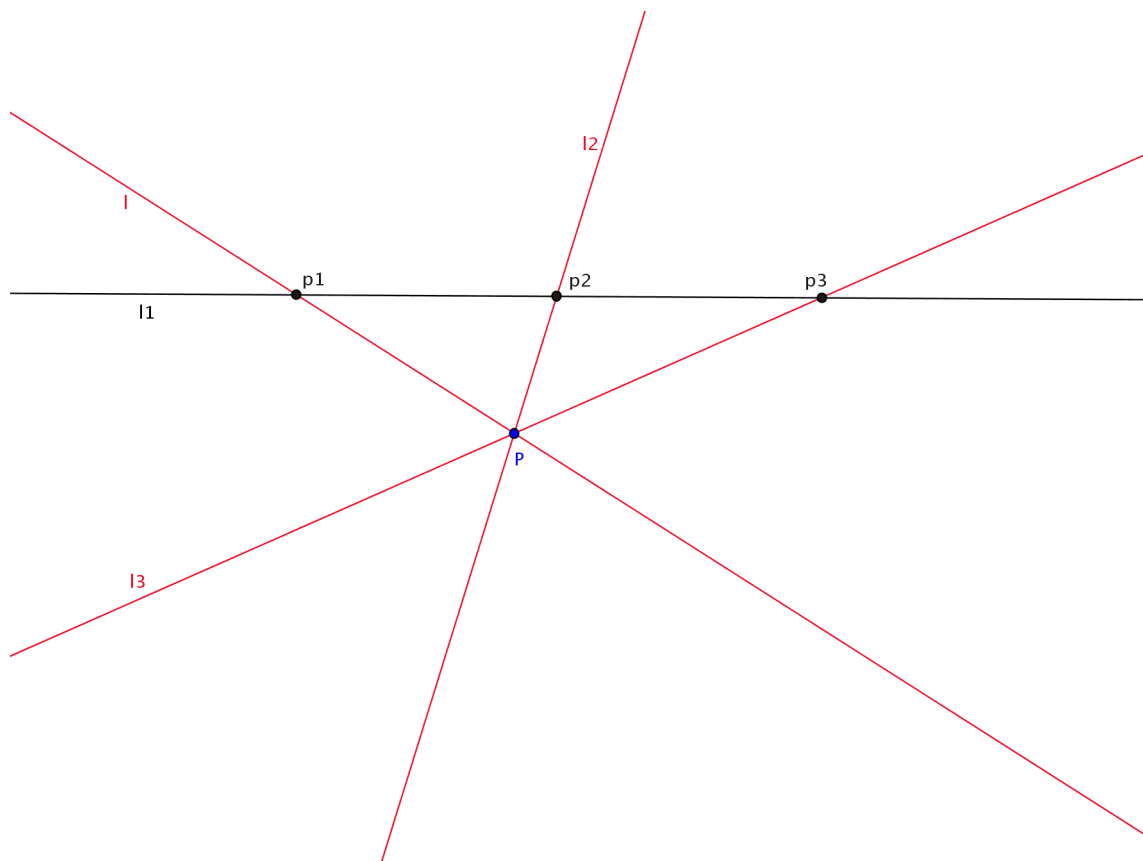


Figura 9.2: Teorema 9.3.2 (DV4)

Ahora probamos, por contradicción, que las tres rectas  $l, l_2, l_3$  son distintas.

Supongamos que  $l = l_2$ . Puesto que  $p_1$  es incidente con  $l$ , obtenemos que  $p_1$  es incidente con  $l_2$ . Además tenemos que  $p_1 \neq p_2$ ,  $p_2$  es incidente con  $l_2$ , y  $p_1, p_2$  son incidentes con  $l_1$ . Luego, por el axioma (V1b), concluimos que  $l_2 = l_1$ . Por lo tanto  $p$  es incidente con  $l_1$ , lo cual es falso.

En forma análoga se demuestra que  $l \neq l_3$  y  $l_2 \neq l_3$ . De esta forma, suponiendo que  $p$  no es incidente con  $l_1$ , hemos demostrado la existencia de tres rectas distintas  $l, l_2, l_3$  que contienen al punto  $p$ .

□

**theorem DV4:**  $\exists l1\ l2\ l3.$

$(l1 \neq l2 \wedge l1 \neq l3 \wedge l2 \neq l3) \wedge$   
 $(incidente\ p\ l1 \wedge incidente\ p\ l2 \wedge incidente\ p\ l3)$

**proof cases** —  $(incidente\ p\ l1)$  o  $\text{no } (incidente\ p\ l1)$

**assume**  $incidente-p-l1: incidente\ p\ l1$

**moreover**

**have**  $\exists p1. \neg incidente\ p1\ l1$  **by** (rule axiomv5)

**then obtain**  $p1$  **where**  $no-incidente-p1-l1: \neg incidente\ p1\ l1$  **by** (rule exE)

**ultimately**

**have**  $distintos-p-p1: p \neq p1$  **by** (rule puntos-distintos)

**hence**  $\exists l2. incidente\ p\ l2 \wedge incidente\ p1\ l2$  **by**(rule mp[OF axiomv1a])

**then obtain**  $l2$  **where**  $incidente-p-l2: incidente\ p\ l2$  **and**  $incidente-p1-l2: incidente\ p1\ l2$

**by auto**

**with**  $no-incidente-p1-l1$

**have**  $incidente\ p1\ l2$  **and**  $\neg incidente\ p1\ l1$  **by simp**

**hence**  $distintas-l2-l1: l2 \neq l1$  **by** (rule lineas-distintas)

**have**  $\exists pa. \neg incidente\ pa\ l2$  **by** (rule axiomv5)

**then obtain**  $pa$  **where**  $no-incidente-pa-l2: \neg incidente\ pa\ l2$  **by** (rule exE)

**with**  $incidente-p1-l2$

**have**  $incidente\ p1\ l2$  **and**  $\neg incidente\ pa\ l2$  **by simp**

**hence**  $distintos-p1-pa: p1 \neq pa$  **by** (rule puntos-distintos)

**hence**  $\exists laux. incidente\ p1\ laux \wedge incidente\ pa\ laux$  **by**(rule mp[OF axiomv1a])

**then obtain**  $laux$  **where**  $incidente-p1-laux: incidente\ p1\ laux$  **and**  $incidente-pa-laux: incidente\ pa\ laux$

**by auto**

**with**  $no-incidente-pa-l2$

**have**  $incidente\ pa\ laux$  **and**  $\neg incidente\ pa\ l2$  **by simp**

**have**  $distintas-laux-l2: laux \neq l2$  **by** (rule lineas-distintas)

**have**  $distintas-laux-l1: laux \neq l1$

**proof** —

**from**  $incidente-p1-laux$  **and**  $no-incidente-p1-l1$

**show**  $?thesis$  **by** (rule lineas-distintas)

**qed**

**have**  $\exists p2. p2 \neq p1 \wedge incidente\ p2\ laux \wedge \neg incidente\ p2\ l1$

**proof** —

**have**  $casos: incidente\ pa\ l1 \vee \neg incidente\ pa\ l1$  **by simp**

**from**  $casos$  **show**  $?thesis$

**proof cases**

**assume**  $incidente-pa-l1: incidente\ pa\ l1$

**have**  $\exists Q1\ Q2\ Q3.$

$Q1 \neq Q2 \wedge Q1 \neq Q3 \wedge$

$Q2 \neq Q3 \wedge incidente\ Q1\ laux \wedge$

*incidente Q2 laux*  $\wedge$  *incidente Q3 laux* **by** (rule axiomv4)  
**then obtain** *Q1 Q2 Q3* **where**  
 $Q1 \neq Q2 \wedge Q1 \neq Q3 \wedge Q2 \neq Q3 \wedge$   
*incidente Q1 laux*  $\wedge$  *incidente Q2 laux*  $\wedge$  *incidente Q3 laux* **by blast**  
**moreover**  
**with** *distintos-p1-pa* **and** *incidente-p1-laux* **and** *incidente-pa-laux*  
**have**  $(Q1=pa \wedge Q2=p1) \vee (Q1=p1 \wedge Q2=pa) \vee$   
 $(Q1=pa \wedge Q3=p1) \vee (Q1=p1 \wedge Q3=pa) \vee$   
 $(Q2=pa \wedge Q3=p1) \vee (Q2=p1 \wedge Q3=pa) \vee$   
 $(Q1 \neq pa \wedge Q1 \neq p1) \vee$   
 $(Q2 \neq pa \wedge Q2 \neq p1) \vee (Q3 \neq pa \wedge Q3 \neq p1)$  **by auto**  
**ultimately**  
**have**  $\exists p2. p2 \neq pa \wedge p2 \neq p1 \wedge$  *incidente p2 laux* **by auto**  
**then obtain** *p2* **where**  
*distintos-p2-pa: p2  $\neq$  pa* **and** *distintos-p2-p1: p2  $\neq$  p1* **and**  
*incidente-p2-laux: incidente p2 laux* **by auto**

**have** *no-incidente-p2-l1:  $\neg$  incidente p2 l1*  
**proof**  
**assume** *incidente p2 l1*  
**with** *distintos-p2-pa* **and** *incidente-pa-l1* **and** *incidente-p2-laux* **and** *incidente-pa-laux*  
**have**  $p2 \neq pa \wedge (incidente p2 l1 \wedge incidente pa l1) \wedge$   
 $(incidente p2 laux \wedge incidente pa laux)$   
**by simp**  
**hence**  $l1=laux$  **by** (rule mp[OF axiomv1b])  
**with** *distintas-laux-l1* **show** *False* **by simp**  
**qed**  
**from** *distintos-p2-p1* **and** *incidente-p2-laux* **and** *no-incidente-p2-l1*  
**show**  $\exists p2. p2 \neq p1 \wedge incidente p2 laux \wedge \neg incidente p2 l1$   
**by auto**  
**next**  
**assume** *no-incidente-pa-l1:  $\neg$  incidente pa l1*  
**with** *distintos-p1-pa* **and** *incidente-pa-laux*  
**show**  $\exists pa. pa \neq p1 \wedge incidente pa laux \wedge \neg incidente pa l1$   
**by auto**  
**qed**  
**qed**  
**then obtain** *p2* **where**  
*distintos-p2-p1: p2  $\neq$  p1* **and** *incidente-p2-laux: incidente p2 laux* **and**  
*no-incidente-p2-l1:  $\neg$  incidente p2 l1* **by auto**  
**have** *distintos-p-p2: p  $\neq$  p2*

**proof**

**assume**  $p=p2$

**with** *incidente-p-l1* **have** *incidente p2 l1* **by** *simp*

**with** *no-incidente-p2-l1* **show** *False* **by** *simp*

**qed**

**hence**  $\exists l3. \textit{incidente } p \textit{ } l3 \wedge \textit{incidente } p2 \textit{ } l3$  **by** (*rule mp[OF axiomv1a]*)

**then obtain** *l3* **where**

*incidente-p-l3: incidente p l3* **and** *incidente-p2-l3: incidente p2 l3* **by** *auto*

**have** *distintas-l3-l1: l3 ≠ l1*

**proof** –

**from** *incidente-p2-l3* **and** *no-incidente-p2-l1*

**show** *?thesis* **by** (*rule lineas-distintas*)

**qed**

**have** *distintas-l3-l2: l3 ≠ l2*

**proof** –

**have** *no-incidente-p2-l2: ¬ incidente p2 l2*

**proof**

**assume** *incidente p2 l2*

**with** *distintos-p2-p1* **and** *incidente-p1-l2* **and** *incidente-p1-laux* **and** *incidente-p2-laux*

**have**  $p1 \neq p2 \wedge (\textit{incidente } p1 \textit{ } l2 \wedge \textit{incidente } p2 \textit{ } l2) \wedge$   
 $(\textit{incidente } p1 \textit{ } laux \wedge \textit{incidente } p2 \textit{ } laux)$  **by** *simp*

**hence**  $l2=laux$  **by** (*rule mp[OF axiomv1b]*)

**with** *distintas-laux-l2* **show** *False* **by** *simp*

**qed**

**from** *incidente-p2-l3* **and** *no-incidente-p2-l2*

**show** *?thesis* **by** (*rule lineas-distintas*)

**qed**

**from** *distintas-l2-l1* **and** *distintas-l3-l1* **and** *distintas-l3-l2* **and**

*incidente-p-l1* **and** *incidente-p-l2* **and** *incidente-p-l3*

**have**  $l1 \neq l2 \wedge l1 \neq l3 \wedge l2 \neq l3 \wedge$

$\textit{incidente } p \textit{ } l1 \wedge \textit{incidente } p \textit{ } l2 \wedge \textit{incidente } p \textit{ } l3$  **by** *simp*

**thus** *?thesis* **by** *auto*

**next**

**assume** *no-incidente-p-l1: ¬ incidente p l1*

**moreover**

**have**  $\exists p1 \textit{ } p2 \textit{ } p3. p1 \neq p2 \wedge p1 \neq p3 \wedge p2 \neq p3 \wedge \textit{incidente } p1 \textit{ } l1$

$\wedge \textit{incidente } p2 \textit{ } l1 \wedge \textit{incidente } p3 \textit{ } l1$  **by** (*rule axiomv4*)

**then obtain**  $p1 \textit{ } p2 \textit{ } p3$  **where**

*distintos-p1-p2: p1 ≠ p2* **and** *distintos-p1-p3: p1 ≠ p3* **and**

*distintos-p2-p3: p2 ≠ p3* **and**

*incidente-p1-l1: incidente p1 l1* **and** *incidente-p2-l1: incidente p2 l1* **and**

*incidente-p3-l1: incidente p3 l1* **by** *auto*

**ultimately**

**have** *distintos-p-p1*:  $p \neq p1$  **and** *distintos-p-p2*:  $p \neq p2$  **and**

*distintos-p-p3*:  $p \neq p3$  **by** *auto*

**from** *distintos-p-p1*

**have**  $\exists l. \textit{incidente } p l \wedge \textit{incidente } p1 l$  **by** (*rule mp[OF axiomv1a]*)

**then obtain** *l* **where**

*incidente-p-l*: *incidente p l* **and** *incidente-p1-l*: *incidente p1 l* **by** *auto*

**from** *distintos-p-p2* **have**  $\exists l2. \textit{incidente } p l2 \wedge \textit{incidente } p2 l2$

**by** (*rule mp[OF axiomv1a]*)

**then obtain** *l2* **where** *incidente-p-l2*: *incidente p l2* **and**

*incidente-p2-l2*: *incidente p2 l2* **by** *auto*

**from** *distintos-p-p3* **have**  $\exists l3. \textit{incidente } p l3 \wedge \textit{incidente } p3 l3$

**by** (*rule mp[OF axiomv1a]*)

**then obtain** *l3* **where**

*incidente-p-l3*: *incidente p l3* **and** *incidente-p3-l3*: *incidente p3 l3* **by** *auto*

**have** *distintas-l-l2*:  $l \neq l2$

**proof**

**assume**  $l=l2$

**with** *incidente-p1-l* **have** *incidente p1 l2* **by** *simp*

**with** *distintos-p1-p2* **and** *incidente-p2-l2* **and** *incidente-p1-l1* **and** *incidente-p2-l1*

**have**  $p1 \neq p2 \wedge (\textit{incidente } p1 l2 \wedge \textit{incidente } p2 l2) \wedge$

$(\textit{incidente } p1 l1 \wedge \textit{incidente } p2 l1)$  **by** *simp*

**hence**  $l2=l1$  **by** (*rule mp[OF axiomv1b]*)

**with** *incidente-p-l2* **have** *incidente p l1* **by** *simp*

**with** *no-incidente-p-l1* **show** *False* **by** *simp*

**qed**

**have** *distintas-l-l3*:  $l \neq l3$

**proof**

**assume**  $l=l3$

**with** *incidente-p1-l* **have** *incidente p1 l3* **by** *simp*

**with** *distintos-p1-p3* **and** *incidente-p3-l3* **and** *incidente-p1-l1* **and** *incidente-p3-l1*

**have**  $p1 \neq p3 \wedge (\textit{incidente } p1 l3 \wedge \textit{incidente } p3 l3) \wedge$

$(\textit{incidente } p1 l1 \wedge \textit{incidente } p3 l1)$  **by** *simp*

**hence**  $l3=l1$  **by** (*rule mp[OF axiomv1b]*)

**with** *incidente-p-l3* **have** *incidente p l1* **by** *simp*

**with** *no-incidente-p-l1* **show** *False* **by** *simp*

**qed**

**have** *distintas-l2-l3*:  $l2 \neq l3$

**proof**

**assume**  $l2=l3$

**with** *incidente-p2-l2* **have** *incidente p2 l3* **by simp**  
**with** *distintos-p2-p3* **and** *incidente-p3-l3* **and** *incidente-p2-l1* **and** *incidente-p3-l1* **have**  
 $p2 \neq p3 \wedge (\text{incidente } p2 \ l3 \wedge \text{incidente } p3 \ l3) \wedge$   
 $(\text{incidente } p2 \ l1 \wedge \text{incidente } p3 \ l1)$  **by simp**  
**hence**  $l3=l1$  **by** (rule *mp*[OF *axiomv1b*])  
**with** *incidente-p-l3* **have** *incidente p l1* **by simp**  
**with** *no-incidente-p-l1* **show** *False* **by simp**  
**qed**

**from** *distintas-l-l2* **and** *distintas-l-l3* **and** *distintas-l2-l3* **and**  
*incidente-p-l* **and** *incidente-p-l2* **and** *incidente-p-l3*  
**have**  $l \neq l2 \wedge l \neq l3 \wedge l2 \neq l3 \wedge$   
 $\text{incidente } p \ l \wedge \text{incidente } p \ l2 \wedge \text{incidente } p \ l3$  **by simp**  
**thus** *?thesis* **by auto**  
**qed**

**Teorema 9.3.3 (DV5)** *No todas las rectas son incidentes con un mismo punto; es decir, dado un punto  $p$  existe una recta  $l$  tal que  $p$  no es incidente con  $l$ .*

**Demostración:** Sea  $p$  un punto cualquiera. Por el principio del tercero excluido se tiene que para cualquier recta  $l$ ,  $p$  es incidente con  $l$  o  $p$  no es incidente con  $l$ . De lo anterior, demostramos por casos el teorema.

1) Supongamos que  $p$  es incidente con  $l$ . Por el axioma (V4) existen tres puntos distintos incidentes con  $l$ , por lo tanto, existe un punto  $q$  incidente con  $l$  y  $p \neq q$ . Además, por el axioma (V5), existe un punto  $r$  que no es incidente con  $l$ , y por lo tanto  $q \neq r$ . Luego, por el axioma (V1a) existe una recta  $l_1$  tal que  $q$  y  $r$  son incidentes con  $l_1$ . Puesto que  $r$  es incidente con  $l_1$  y no es incidente con  $l$  tenemos que  $l_1 \neq l$  (ver Figura 9.3).

De lo anterior concluimos que  $p$  no es incidente con  $l_1$ , ya que en el caso contrario, usando  $q \neq p$ ,  $q$  incidente con  $l_1$ , y  $p, q$  incidentes con  $l$ , tenemos por el axioma (V1b) que  $l_1 = l$ , lo cual es falso. De esta forma queda demostrado el teorema.

2) Supongamos que  $p$  no es incidente con  $l$ . Entonces no hay nada por demostrar. □

**theorem** *DV5*:  $\exists l. \neg \text{incidente } p \ l$

**proof** –

**have** *casos*:  $\text{incidente } p \ l \vee \neg \text{incidente } p \ l$  **by simp**

**from** *casos* **show** *?thesis*

**proof** *cases*

**assume** *incidente-p-l*:  $\text{incidente } p \ l$

**have**  $\exists Q1 \ Q2 \ Q3.$

$Q1 \neq Q2 \wedge Q1 \neq Q3 \wedge$



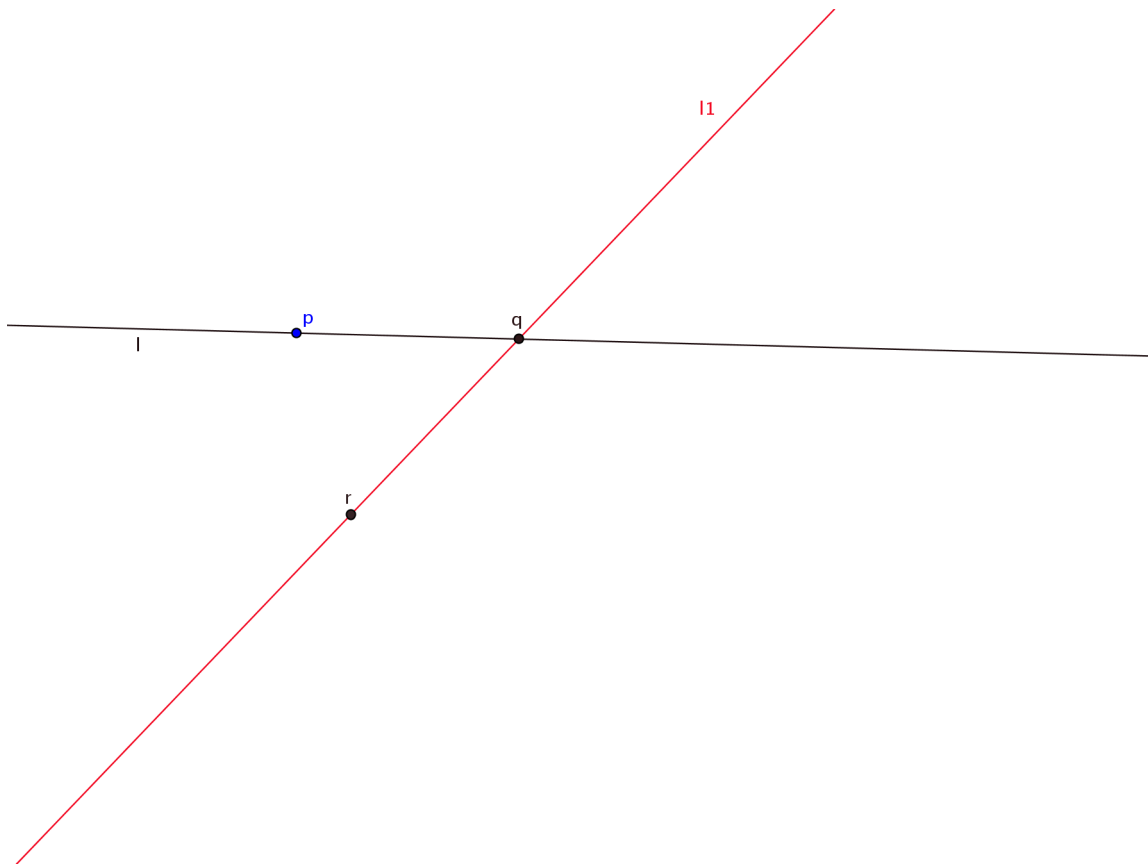


Figura 9.3: Teorema 9.3.3 (DV5)

$Q2 \neq Q3 \wedge \text{incidente } Q1 \ l \wedge$   
 $\text{incidente } Q2 \ l \wedge \text{incidente } Q3 \ l$  **by** (rule axiomv4)  
**then obtain**  $Q1 \ Q2 \ Q3$  **where**  
 $Q1 \neq Q2 \wedge Q1 \neq Q3 \wedge Q2 \neq Q3 \wedge$   
 $\text{incidente } Q1 \ l \wedge \text{incidente } Q2 \ l \wedge \text{incidente } Q3 \ l$  **by blast**

**moreover**

**with** *incidente-p-l*

**have**  $(Q1 = p \wedge Q2 \neq p) \vee (Q1 \neq p \wedge Q2 = p) \vee$   
 $(Q1 = p \wedge Q3 \neq p) \vee (Q1 \neq p \wedge Q3 = p) \vee$   
 $(Q2 = p \wedge Q3 \neq p) \vee (Q2 \neq p \wedge Q3 = p) \vee$   
 $(Q1 \neq p \wedge Q2 \neq p \wedge Q3 \neq p)$  **by auto**

**ultimately**

**have**  $\exists q. q \neq p \wedge \text{incidente } q \ l$  **by auto**

**then obtain**  $q$  **where**

*distintos-q-p:  $q \neq p$  and incidente-q-l: incidente  $q \ l$*  **by auto**

**have**  $\exists r. \neg \text{incidente } r \ l$  **by** (rule axiomv5)

**then obtain**  $r$  **where** *no-incidente-r-l:  $\neg \text{incidente } r \ l$*  **by** (rule exE)

**with** *incidente-q-l*

**have** *incidente  $q \ l$  and  $\neg \text{incidente } r \ l$*  **by simp**

**hence** *distintos-q-r:  $q \neq r$*  **by** (rule puntos-distintos)

**hence**  $\exists l1. \text{incidente } q \ l1 \wedge \text{incidente } r \ l1$  **by** (rule mp[OF axiomv1a])

**then obtain**  $l1$  **where** *incidente-q-l1: incidente  $q \ l1$  and incidente-r-l1: incidente  $r \ l1$*

**by auto**

**with** *no-incidente-r-l*

**have** *incidente  $r \ l1$  and  $\neg \text{incidente } r \ l$*  **by simp**

**hence** *distintas-l1-l:  $l1 \neq l$*  **by** (rule lineas-distintas)

**have** *no-incidente-p-l1:  $\neg \text{incidente } p \ l1$*

**proof**

**assume** *incidente  $p \ l1$*

**with** *distintos-q-p and incidente-q-l1 and incidente-p-l and incidente-q-l*

**have**  $q \neq p \wedge (\text{incidente } q \ l1 \wedge \text{incidente } p \ l1) \wedge$

$(\text{incidente } q \ l \wedge \text{incidente } p \ l)$  **by simp**

**hence**  $l1 = l$  **by** (rule mp[OF axiomv1b])

**with** *distintas-l1-l show False* **by simp**

**qed**

**thus** *?thesis* **by auto**

**next**

**assume**  *$\neg \text{incidente } p \ l$*

**thus** *?thesis ..*

**qed**

**qed**

La manera como se obtuvieron los teoremas (DV4) y (DV5) a partir de (V4) y (V5) respectivamente, son un caso particular del siguiente principio.

### Principio de dualidad

Si en los axiomas (V1a), (V1b), (V2), (V4), (V5), intercambiamos las palabras “punto” y “recta”, obtenemos (V2), (DV1b), (V1a), (DV4) y (DV5) respectivamente.

Sea  $P$  una prueba de un teorema  $T$  a partir de (V1a), (V1b), (V2), (V4), (V5). Si intercambiamos “punto” y “recta” en  $P$  y en  $T$  obteniendo  $P'$  y  $T'$  respectivamente, tenemos que  $P'$  es una demostración de  $T'$  a partir de (V2), (DV1b), (V1a), (DV4) y (DV5).

Puesto que, (DV1b), (DV4) y (DV5) se han demostrado a partir de (V1a), (V1b), (V2), (V4), (V5), tenemos en total que  $T'$  se ha demostrado a partir de (V1a), (V1b), (V2), (V4), (V5)  $T'$ .

De esta forma, obtenemos el siguiente *principio de dualidad*: sea  $T$  un teorema de la geometría proyectiva, y  $T'$  la frase que resulta al intercambiar las palabras “punto” y “recta” en  $T$ . Entonces,  $T'$  es un teorema de la geometría proyectiva.  $T$  y  $T'$  son llamados teoremas duales.

### Dos sistemas de axiomas para la geometría proyectiva

Los conjuntos  $S_1 = \{V1a, V1b, V2, V3\}$  y  $S_2 = \{V1a, V1b, V2, V4, V5\}$  forman dos sistemas de axiomas para la geometría proyectiva.  $S_2$  se obtiene a partir de  $S_1$  sustituyendo (V3) por (V4) y (V5), y viceversa. En lo que sigue probamos parte de esta equivalencia demostrando como un teorema el axioma (V3) en  $S_2$ . Para esto, utilizamos el siguiente lema.

**Lema 9.3.4 (laxiomv3)** *Existen cuatro puntos distintos  $p_1, p_2, p_3, p_4$  y cuatro rectas  $l_1, l_2, l_3, l_4$ , tales que  $l_1$  y  $l_4$  son diferentes de  $l_2$  y  $l_3$ ;  $p_1$  y  $p_2$  son incidentes con  $l_1$ ;  $p_1$  y  $p_4$  son incidentes con  $l_2$ ;  $p_2$  y  $p_3$  son incidentes con  $l_3$ ;  $p_3$  y  $p_4$  son incidentes con  $l_4$  (ver Figura 9.4).*

**Demostración:** Sea  $l_{a1}$  una recta cualquiera. Por el axioma (V4) existen tres puntos distintos  $p_1, p_a, p_3$  incidentes con  $l_{a1}$ , además por el axioma (V5) existe un punto  $p_4$  que no es incidente con  $l_{a1}$  (ver Figura 9.5).

De lo anterior se concluye que  $p_1, p_a, p_3$  son distintos de  $p_4$ . Por lo tanto, por el axioma (V1a), existen rectas  $l_{a2}, l_2, l_4$  tales que,  $p_a$  y  $p_4$  son incidentes con  $l_{a2}$ ;  $p_1$  y  $p_4$  son incidentes con  $l_2$ ;  $p_3$  y  $p_4$  son incidentes con  $l_4$  (ver Figura 9.6).

Hasta aquí tenemos que existen tres puntos distintos  $p_1, p_3, p_4$  y dos rectas  $l_2, l_4$  tales que  $p_1$  y  $p_4$  son incidentes con  $l_2$ , y  $p_3$  y  $p_4$  incidentes con  $l_4$ .

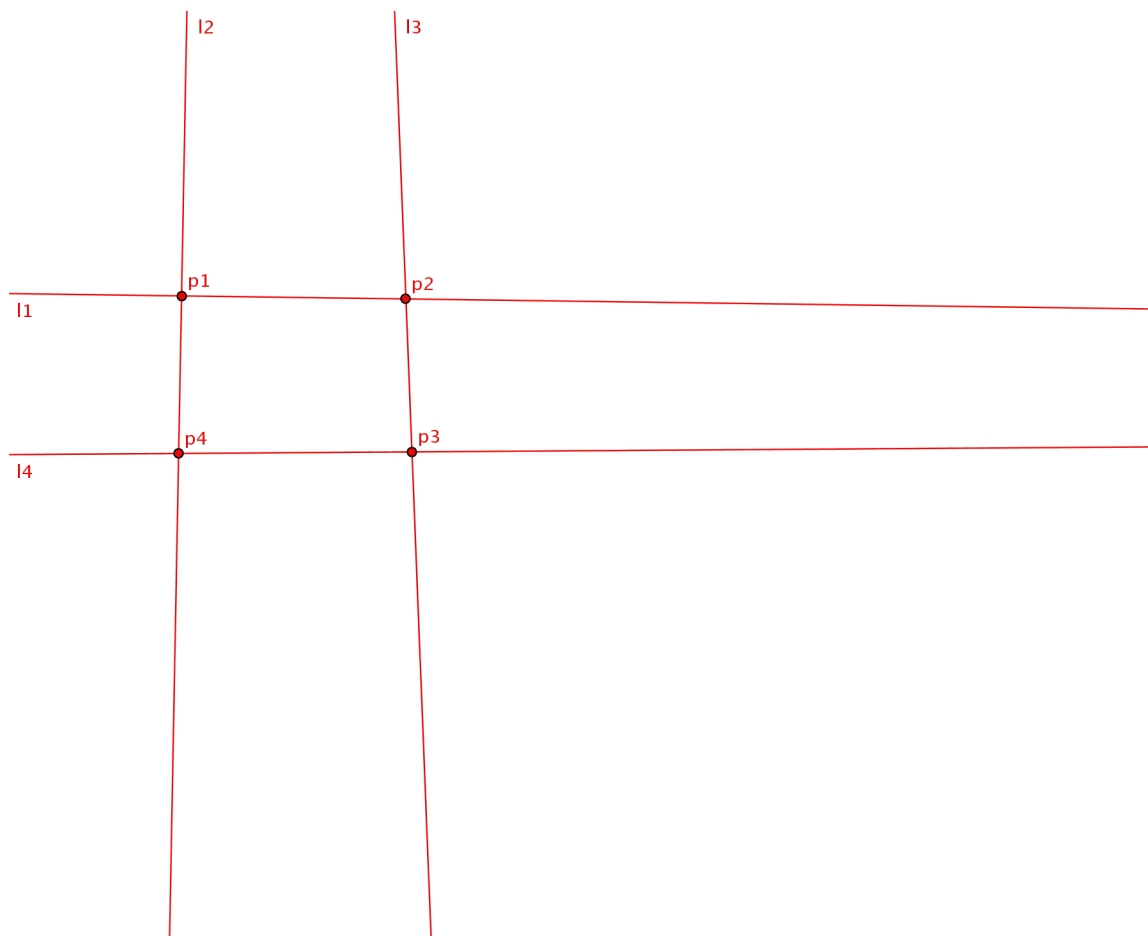


Figura 9.4: Teorema 9.3.4

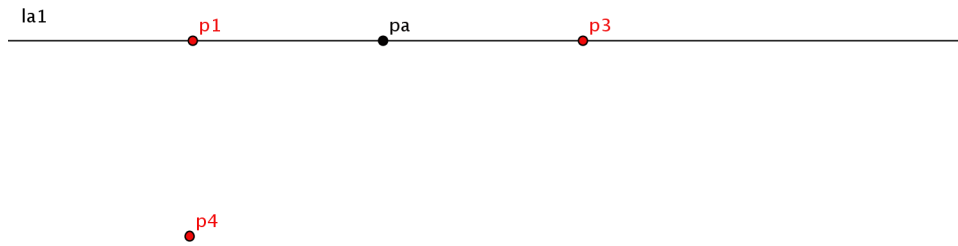


Figura 9.5: Teorema 9.3.4

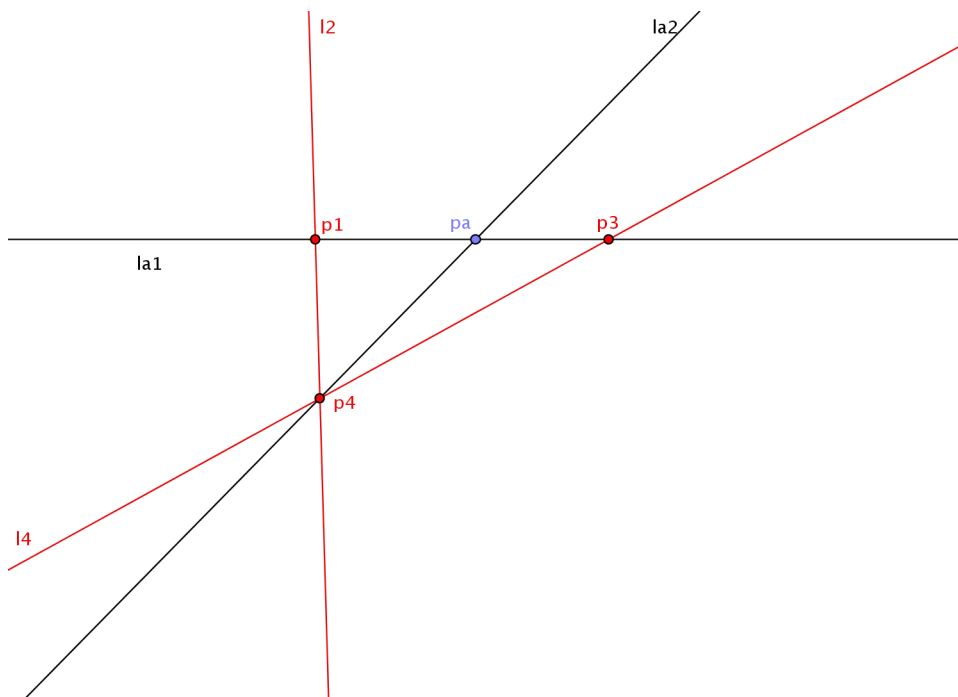


Figura 9.6: Teorema 9.3.4

Ahora mostramos que existe un punto  $p_2$  y dos rectas  $l_1, l_3$  tales que,  $p_2 \neq p_1, p_3, p_4$ ;  $p_1$  y  $p_2$  son incidentes con  $l_1$ ;  $p_2$  y  $p_3$  son incidentes con  $l_3$  (ver Figura 9.7).

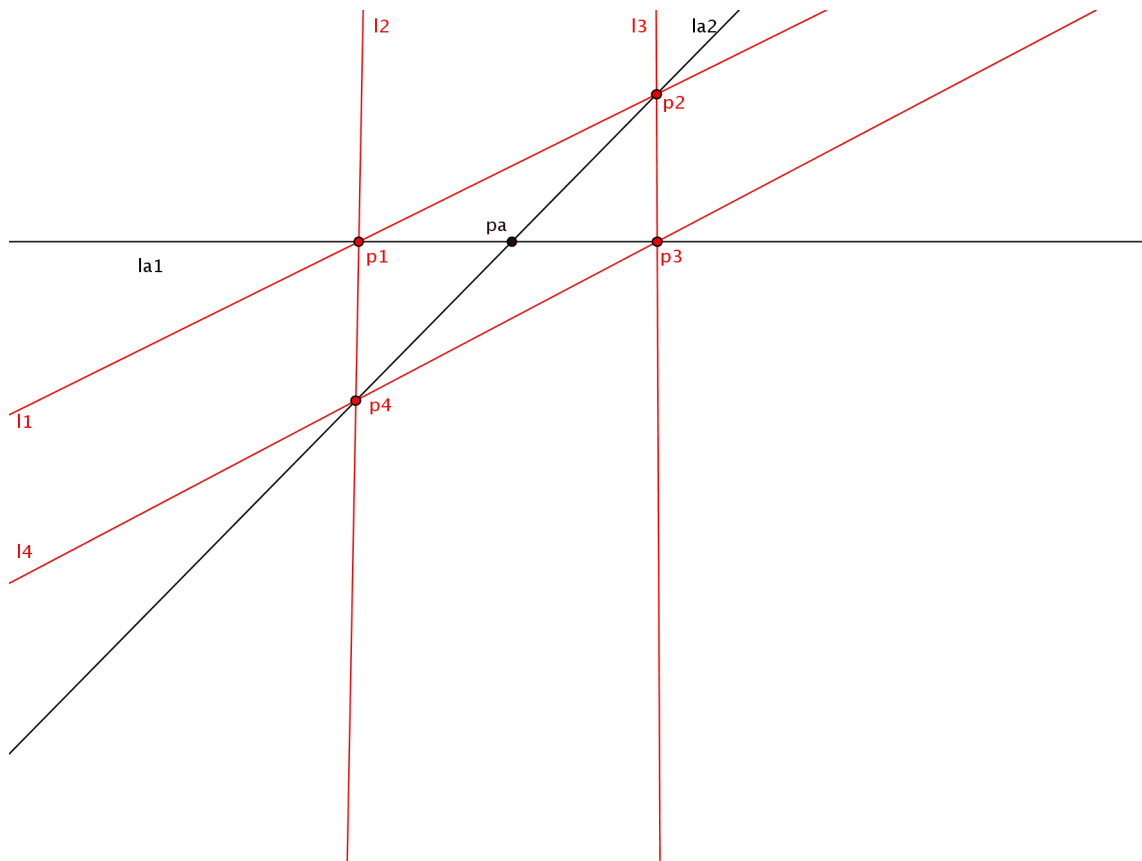


Figura 9.7: Teorema 9.3.4

Puesto que  $p_4$  es incidente con  $l_{a2}$  y no es incidente con  $l_{a1}$ , tenemos que  $l_{a1} \neq l_{a2}$ .

Por el axioma (V4) existen tres puntos distintos incidentes con  $l_{a2}$  y puesto que  $p_a$  y  $p_4$  son puntos distintos e incidentes con  $l_{a2}$ , se concluye que existe  $p_2$  distinto de  $p_a$  y  $p_4$  incidente con  $l_{a2}$ .

Usando  $l_{a1} \neq l_{a2}$  se tiene que  $p_1 \neq p_2$ : supongamos que  $p_1 = p_2$  entonces, como  $p_2$  es incidente con  $l_{a2}$ , tenemos que  $p_1$  es incidente con  $l_{a2}$ , además sabemos que,  $p_1 \neq p_a$ ;  $p_a$  es incidente con  $l_{a2}$ ;  $p_1, p_a$  son incidentes con  $l_{a1}$ . Por lo tanto, por el axioma (V1b), obtenemos  $l_{a1} = l_{a2}$  lo cual es falso. Análogamente, usando  $l_{a1} \neq l_{a2}$ , se demuestra que  $p_2 \neq p_3$ .

A partir de  $p_1 \neq p_2$ , por el axioma (V1a), obtenemos una recta  $l_1$  tal que  $p_1$  y  $p_2$  son incidentes con  $l_1$ . De la misma forma, a partir de  $p_2 \neq p_3$  obtenemos una recta  $l_3$  tal que  $p_2$  y  $p_3$  son incidentes con  $l_3$ .

Falta por demostrar que  $l_1$  y  $l_4$  son diferentes de  $l_2$  y  $l_3$ . Puesto que  $p_4$  no es incidente

con  $l_{a1}$  y es incidente con  $l_4$  tenemos que  $l_{a1} \neq l_4$ . De esto último demostramos que  $l_4 \neq l_2$ . Supongamos que  $l_4 = l_2$  entonces, como  $p_1$  es incidente con  $l_2$ , tenemos que  $p_1$  es incidente con  $l_4$ , además sabemos que,  $p_1 \neq p_3$ ;  $p_3$  es incidente con  $l_4$ ;  $p_1, p_3$  son incidentes con  $l_{a1}$ ; Por lo tanto, por el axioma (V1b), obtenemos que  $l_{a1} = l_4$  lo cual es falso.

Siguiendo el mismo raciocinio utilizado en la demostración anterior, usando  $l_{a1} \neq l_{a2}$  se demuestra que  $l_{a1} \neq l_1$ ,  $l_{a2} \neq l_1$  y  $l_{a2} \neq l_4$ .

De igual forma, usando  $l_{a1} \neq l_1$  se demuestra que  $l_1 \neq l_3$ , usando  $l_{a2} \neq l_1$  se demuestra que  $l_1 \neq l_2$  y usando  $l_{a2} \neq l_2$  se demuestra que  $l_4 \neq l_3$ . De esta forma queda demostrado el lema. □

**lemma** *axiomv3*:

$\exists p1 p2 p3 p4 l1 l2 l3 l4.$   
 $p1 \neq p2 \wedge p1 \neq p3 \wedge p1 \neq p4 \wedge p2 \neq p3 \wedge p2 \neq p4 \wedge p3 \neq p4 \wedge$   
 $l1 \neq l2 \wedge l1 \neq l3 \wedge l4 \neq l2 \wedge l4 \neq l3 \wedge$   
*(incidente p1 l1  $\wedge$  incidente p2 l1)  $\wedge$*   
*(incidente p1 l2  $\wedge$  incidente p4 l2)  $\wedge$*   
*(incidente p2 l3  $\wedge$  incidente p3 l3)  $\wedge$*   
*(incidente p3 l4  $\wedge$  incidente p4 l4)*

**proof** –

**from** *axiomv4*

**have**  $\exists p1 pa p3. p1 \neq pa \wedge p1 \neq p3 \wedge pa \neq p3 \wedge$   
*incidente p1 la1  $\wedge$  incidente pa la1  $\wedge$  incidente p3 la1* **by simp**

**then obtain**  $p1 pa p3$  **where**

*distintos-p1-pa: p1  $\neq$  pa* **and** *distintos-p1-p3: p1  $\neq$  p3* **and**

*distintos-pa-p3: pa  $\neq$  p3* **and**

*incidente-p1-la1: incidente p1 la1* **and** *incidente-pa-la1: incidente pa la1* **and**

*incidente-p3-la1: incidente p3 la1* **by auto**

**moreover**

**from** *axiomv5* **have**  $\exists p4. \neg$ *incidente p4 la1* **by simp**

**then obtain**  $p4$  **where** *no-incidente-p4-la1:  $\neg$ incidente p4 la1* **by** (rule *exE*)

**ultimately**

**have** *distintos-p1-p4: p1  $\neq$  p4* **and** *distintos-pa-p4: pa  $\neq$  p4* **and**

*distintos-p3-p4: p3  $\neq$  p4* **by auto**

**from** *distintos-pa-p4* **have**

$\exists la2. incidente pa la2 \wedge incidente p4 la2$  **by** (rule *mp*[OF *axiomv1a*])

**then obtain**  $la2$  **where** *incidente-pa-la2: incidente pa la2* **and**

*incidente-p4-la2: incidente p4 la2* **by auto**

**from** *distintos-p1-p4* **have**

$\exists l2$ . *incidente*  $p1\ l2 \wedge$  *incidente*  $p4\ l2$  **by** (rule *mp*[OF *axiomv1a*])

**then obtain**  $l2$  **where** *incidente-p1-l2*:*incidente*  $p1\ l2$  **and**

*incidente-p4-l2*:*incidente*  $p4\ l2$  **by** *auto*

**from** *distintos-p3-p4* **have**

$\exists l4$ . *incidente*  $p3\ l4 \wedge$  *incidente*  $p4\ l4$  **by** (rule *mp*[OF *axiomv1a*])

**then obtain**  $l4$  **where** *incidente-p3-l4*: *incidente*  $p3\ l4$  **and**

*incidente-p4-l4*: *incidente*  $p4\ l4$  **by** *auto*

**from** *axiomv4* **have**  $\exists Q1\ Q2\ Q3$ .

$Q1 \neq Q2 \wedge Q1 \neq Q3 \wedge$

$Q2 \neq Q3 \wedge$  *incidente*  $Q1\ la2 \wedge$

*incidente*  $Q2\ la2 \wedge$  *incidente*  $Q3\ la2$  **by** *simp*

**then obtain**  $Q1\ Q2\ Q3$  **where**

$Q1 \neq Q2 \wedge Q1 \neq Q3 \wedge Q2 \neq Q3 \wedge$

*incidente*  $Q1\ la2 \wedge$  *incidente*  $Q2\ la2 \wedge$  *incidente*  $Q3\ la2$  **by** *blast*

**moreover**

**with** *distintos-pa-p4* **and** *incidente-pa-la2* **and** *incidente-p4-la2*

**have**  $(Q1=pa \wedge Q2=p4) \vee (Q1=p4 \wedge Q2=pa) \vee$

$(Q1=pa \wedge Q3=p4) \vee (Q1=p4 \wedge Q3=pa) \vee$

$(Q2=pa \wedge Q3=p4) \vee (Q2=p4 \wedge Q3=pa) \vee$

$(Q1 \neq pa \wedge Q1 \neq p4) \vee$

$(Q2 \neq pa \wedge Q2 \neq p4) \vee (Q3 \neq pa \wedge Q3 \neq p4)$  **by** *auto*

**ultimately**

**have**  $\exists p2$ .  $p2 \neq pa \wedge p2 \neq p4 \wedge$  *incidente*  $p2\ la2$  **by** *auto*

**then obtain**  $p2$  **where**

*distintos-p2-pa*:  $p2 \neq pa$  **and** *distintos-p2-p4*:  $p2 \neq p4$  **and**

*incidente-p2-la2*: *incidente*  $p2\ la2$  **by** *auto*

**have** *distintas-la1-la2*:  $la1 \neq la2$

**proof**

**assume**  $la1 = la2$

**with** *incidente-p4-la2*

**have** *incidente*  $p4\ la1$  **by** *simp*

**with** *no-incidente-p4-la1* **show** *False* **by** *simp*

**qed**

**have** *distintos-p1-p2*:  $p1 \neq p2$

**proof**

**assume**  $p1 = p2$

**with** *incidente-p2-la2*

**have** *incidente-p1-la2*: *incidente*  $p1\ la2$  **by** *simp*

**with** *distintos-p1-pa* **and** *incidente-pa-la2* **and** *incidente-p1-la1* **and** *incidente-pa-la1*



**have**  $p1 \neq pa \wedge (\text{incidente } p1 \text{ } la1 \wedge \text{incidente } pa \text{ } la1) \wedge$   
 $(\text{incidente } p1 \text{ } la2 \wedge \text{incidente } pa \text{ } la2)$  **by simp**  
**hence**  $la1 = la2$  **by**  $(\text{rule mp}[\text{OF axiomv1b}])$   
**with** *distintas-la1-la2* **show** *False* **by simp**  
**qed**  
**hence**  $\exists l1. \text{incidente } p1 \text{ } l1 \wedge \text{incidente } p2 \text{ } l1$  **by**  $(\text{rule mp}[\text{OF axiomv1a}])$   
**then obtain** *l1* **where** *incidente-p1-l1: incidente p1 l1* **and**  
*incidente-p2-l1: incidente p2 l1* **by auto**

**have** *distintos-p2-p3: p2 ≠ p3*  
**proof**  
**assume**  $p2 = p3$   
**with** *incidente-p2-la2*  
**have** *incidente-p3-la2: incidente p3 la2* **by simp**  
**with** *distintos-pa-p3* **and** *incidente-pa-la2* **and** *incidente-pa-la1* **and** *incidente-p3-la1*  
**have**  $pa \neq p3 \wedge (\text{incidente } pa \text{ } la1 \wedge \text{incidente } p3 \text{ } la1) \wedge$   
 $(\text{incidente } pa \text{ } la2 \wedge \text{incidente } p3 \text{ } la2)$  **by simp**  
**hence**  $la1 = la2$  **by**  $(\text{rule mp}[\text{OF axiomv1b}])$   
**with** *distintas-la1-la2* **show** *False* **by simp**  
**qed**  
**hence**  $\exists l3. \text{incidente } p2 \text{ } l3 \wedge \text{incidente } p3 \text{ } l3$  **by**  $(\text{rule mp}[\text{OF axiomv1a}])$   
**then obtain** *l3* **where** *incidente-p2-l3: incidente p2 l3* **and**  
*incidente-p3-l3: incidente p3 l3* **by auto**

**have** *distintas-la1-l4: la1 ≠ l4*  
**proof**  
**assume**  $la1 = l4$   
**with** *incidente-p4-l4*  
**have** *incidente p4 la1* **by simp**  
**with** *no-incidente-p4-la1* **show** *False* **by simp**  
**qed**

**have** *distintas-l4-l2: l4 ≠ l2*  
**proof**  
**assume**  $l4 = l2$   
**with** *incidente-p1-l2*  
**have** *incidente p1 l4* **by simp**  
**with** *distintos-p1-p3* **and** *incidente-p3-l4* **and** *incidente-p1-la1* **and** *incidente-p3-la1*  
**have**  $p1 \neq p3 \wedge (\text{incidente } p1 \text{ } la1 \wedge \text{incidente } p3 \text{ } la1) \wedge$   
 $(\text{incidente } p1 \text{ } l4 \wedge \text{incidente } p3 \text{ } l4)$  **by simp**  
**hence**  $la1 = l4$  **by**  $(\text{rule mp}[\text{OF axiomv1b}])$   
**with** *distintas-la1-l4* **show** *False* **by simp**  
**qed**

**have** *distintas-la1-l1:la1≠l1*  
**proof**  
**assume**  $la1 = l1$   
**with** *incidente-p2-l1*  
**have** *incidente p2 la1* **by** *simp*  
**with** *distintos-p2-pa* **and** *incidente-pa-la1* **and** *incidente-p2-la2* **and** *incidente-pa-la2*  
**have**  $p2 \neq pa \wedge (incidente\ p2\ la1 \wedge incidente\ pa\ la1) \wedge$   
 $(incidente\ p2\ la2 \wedge incidente\ pa\ la2)$  **by** *simp*  
**hence**  $la1 = la2$  **by** (*rule mp[OF axiomv1b]*)  
**with** *distintas-la1-la2* **show** *False* **by** *simp*  
**qed**

**have** *distintas-la2-l1:la2≠l1*  
**proof**  
**assume**  $la2 = l1$   
**with** *incidente-p1-l1*  
**have** *incidente p1 la2* **by** *simp*  
**with** *distintos-p1-pa* **and** *incidente-pa-la2* **and** *incidente-p1-la1* **and** *incidente-pa-la1*  
**have**  $p1 \neq pa \wedge (incidente\ p1\ la1 \wedge incidente\ pa\ la1) \wedge$   
 $(incidente\ p1\ la2 \wedge incidente\ pa\ la2)$  **by** *simp*  
**hence**  $la1 = la2$  **by** (*rule mp[OF axiomv1b]*)  
**with** *distintas-la1-la2* **show** *False* **by** *simp*  
**qed**

**have** *distintas-l1-l3:l1≠l3*  
**proof**  
**assume**  $l1 = l3$   
**with** *incidente-p3-l3*  
**have** *incidente p3 l1* **by** *simp*  
**with** *distintos-p1-p3* **and** *incidente-p1-l1* **and** *incidente-p1-la1* **and** *incidente-p3-la1*  
**have**  $p1 \neq p3 \wedge (incidente\ p1\ la1 \wedge incidente\ p3\ la1) \wedge$   
 $(incidente\ p1\ l1 \wedge incidente\ p3\ l1)$  **by** *simp*  
**hence**  $la1 = l1$  **by** (*rule mp[OF axiomv1b]*)  
**with** *distintas-la1-l1* **show** *False* **by** *simp*  
**qed**

**have** *distintas-l1-l2:l1≠l2*  
**proof**  
**assume**  $l1 = l2$   
**with** *incidente-p4-l2*  
**have** *incidente p4 l1* **by** *simp*  
**with** *distintos-p2-p4* **and** *incidente-p2-l1* **and** *incidente-p2-la2* **and** *incidente-p4-la2*

**have**  $p_2 \neq p_4 \wedge (\text{incidente } p_2 \text{ } l_2 \wedge \text{incidente } p_4 \text{ } l_2) \wedge$   
 $(\text{incidente } p_2 \text{ } l_1 \wedge \text{incidente } p_4 \text{ } l_1)$  **by simp**  
**hence**  $l_2 = l_1$  **by** (rule mp[OF axiomv1b])  
**with** *distintas- $l_2$ - $l_1$*  **show** False **by simp**  
**qed**

**have** *distintas- $l_2$ - $l_4$* :  $l_2 \neq l_4$

**proof**

**assume**  $l_2 = l_4$

**with** *incidente- $p_3$ - $l_4$*

**have** *incidente- $p_3$ - $l_2$*  **by simp**

**with** *distintos- $p_a$ - $p_3$*  **and** *incidente- $p_a$ - $l_2$*  **and** *incidente- $p_3$ - $l_1$*  **and** *incidente- $p_a$ - $l_1$*

**have**  $p_3 \neq p_a \wedge (\text{incidente } p_3 \text{ } l_1 \wedge \text{incidente } p_a \text{ } l_1) \wedge$

$(\text{incidente } p_3 \text{ } l_2 \wedge \text{incidente } p_a \text{ } l_2)$  **by simp**

**hence**  $l_1 = l_2$  **by** (rule mp[OF axiomv1b])

**with** *distintas- $l_1$ - $l_2$*  **show** False **by simp**

**qed**

**have** *distintas- $l_4$ - $l_3$* :  $l_4 \neq l_3$

**proof**

**assume**  $l_4 = l_3$

**with** *incidente- $p_2$ - $l_3$*

**have** *incidente- $p_2$ - $l_4$*  **by simp**

**with** *distintos- $p_2$ - $p_4$*  **and** *incidente- $p_4$ - $l_4$*  **and** *incidente- $p_2$ - $l_2$*  **and** *incidente- $p_4$ - $l_2$*

**have**  $p_2 \neq p_4 \wedge (\text{incidente } p_2 \text{ } l_2 \wedge \text{incidente } p_4 \text{ } l_2) \wedge$

$(\text{incidente } p_2 \text{ } l_4 \wedge \text{incidente } p_4 \text{ } l_4)$  **by simp**

**hence**  $l_2 = l_4$  **by** (rule mp[OF axiomv1b])

**with** *distintas- $l_2$ - $l_4$*  **show** False **by simp**

**qed**

**from** *distintos- $p_1$ - $p_2$*  **and** *distintos- $p_1$ - $p_3$*  **and** *distintos- $p_1$ - $p_4$*  **and**

*distintos- $p_2$ - $p_3$*  **and** *distintos- $p_2$ - $p_4$*  **and** *distintos- $p_3$ - $p_4$*  **and**

*distintas- $l_1$ - $l_2$*  **and** *distintas- $l_1$ - $l_3$*  **and** *distintas- $l_4$ - $l_2$*  **and** *distintas- $l_4$ - $l_3$*  **and**

*incidente- $p_1$ - $l_1$*  **and** *incidente- $p_2$ - $l_1$*  **and** *incidente- $p_1$ - $l_2$*  **and** *incidente- $p_4$ - $l_2$*  **and**

*incidente- $p_2$ - $l_3$*  *incidente- $p_3$ - $l_3$*  **and** *incidente- $p_3$ - $l_4$*  **and** *incidente- $p_4$ - $l_4$*

**show** ?thesis **by blast**

**qed**

**Teorema 9.3.5 (axiomv3)** *Existen por lo menos cuatro puntos tales que ninguna recta pasa por tres de ellos. Es decir, existen cuatro puntos distintos  $p_1, p_2, p_3, p_4$  tal que para toda recta  $l$ ,*

$\neg(p_1 \text{ es incidente con } l \wedge p_2 \text{ es incidente con } l \wedge p_3 \text{ es incidente con } l) \wedge$

$\neg(p_1 \text{ es incidente con } l \wedge p_2 \text{ es incidente con } l \wedge p_4 \text{ es incidente con } l) \wedge$

$\neg(p_1 \text{ es incidente con } l \wedge p_3 \text{ es incidente con } l \wedge p_4 \text{ es incidente con } l) \wedge$   
 $\neg(p_2 \text{ es incidente con } l \wedge p_3 \text{ es incidente con } l \wedge p_4 \text{ es incidente con } l).$

**Demostración:** Por el lema 9.3.4, existen cuatro puntos distintos  $p_1, p_2, p_3, p_4$  y cuatro rectas  $l_1, l_2, l_3, l_4$ , tales que

$l_1$  y  $l_4$  son diferentes de  $l_2$  y  $l_3$ ;  $p_1$  y  $p_2$  son incidentes con  $l_1$ ;  $p_1$  y  $p_4$  son incidentes con  $l_2$ ;  $p_2$  y  $p_3$  son incidentes con  $l_3$ ;  $p_3$  y  $p_4$  son incidentes con  $l_4$ .

Probemos que estos cuatro puntos  $p_1, p_2, p_3, p_4$  cumplen las propiedades del teorema, es decir, demostremos que  $p_1, p_2, p_3, p_4$  son distintos y para toda recta  $l$  se tiene que,

$\neg((p_1 \text{ es incidente con } l \wedge p_2 \text{ es incidente con } l \wedge p_3 \text{ es incidente con } l) \vee$   
 $(p_1 \text{ es incidente con } l \wedge p_2 \text{ es incidente con } l \wedge p_4 \text{ es incidente con } l) \vee$   
 $(p_1 \text{ es incidente con } l \wedge p_3 \text{ es incidente con } l \wedge p_4 \text{ es incidente con } l) \vee$   
 $(p_2 \text{ es incidente con } l \wedge p_3 \text{ es incidente con } l \wedge p_4 \text{ es incidente con } l)).$

Por el lema 9.3.4,  $p_1, p_2, p_3, p_4$  son distintos. Ahora, sea  $l$  una recta cualquiera. Supongamos que

$(p_1 \text{ es incidente con } l \wedge p_2 \text{ es incidente con } l \wedge p_3 \text{ es incidente con } l) \vee$   
 $(p_1 \text{ es incidente con } l \wedge p_2 \text{ es incidente con } l \wedge p_4 \text{ es incidente con } l) \vee$   
 $(p_1 \text{ es incidente con } l \wedge p_3 \text{ es incidente con } l \wedge p_4 \text{ es incidente con } l) \vee$   
 $(p_2 \text{ es incidente con } l \wedge p_3 \text{ es incidente con } l \wedge p_4 \text{ es incidente con } l)$

y obtengamos, para cada caso, una contradicción.

Supongamos que,  $(p_1 \text{ es incidente con } l \wedge p_2 \text{ es incidente con } l \wedge p_3 \text{ es incidente con } l)$ .

Por el lema 9.3.4 tenemos que,  $p_1$  y  $p_2$  son distintos e incidentes con  $l_1$ , y  $p_2$  y  $p_3$  son distintos e incidentes con  $l_3$ . Por lo tanto, por el axioma (V1b),  $l_1 = l = l_3$  y por el lema 9.3.4,  $l_1 \neq l_3$ . De esta forma obtenemos una contradicción. De igual forma, se demuestran los otros casos.

□

**theorem axiomv3:**

$\exists p_1 p_2 p_3 p_4. p_1 \neq p_2 \wedge p_1 \neq p_3 \wedge p_1 \neq p_4 \wedge p_2 \neq p_3 \wedge p_2 \neq p_4 \wedge p_3 \neq p_4 \wedge$   
 $(\forall l. \neg(\text{incidente } p_1 l \wedge \text{incidente } p_2 l \wedge \text{incidente } p_3 l)) \wedge$   
 $\neg(\text{incidente } p_1 l \wedge \text{incidente } p_2 l \wedge \text{incidente } p_4 l) \wedge$   
 $\neg(\text{incidente } p_1 l \wedge \text{incidente } p_3 l \wedge \text{incidente } p_4 l) \wedge$   
 $\neg(\text{incidente } p_2 l \wedge \text{incidente } p_3 l \wedge \text{incidente } p_4 l))$

**proof** –

**have**  $\exists p_1 p_2 p_3 p_4 l_1 l_2 l_3 l_4.$   
 $p_1 \neq p_2 \wedge p_1 \neq p_3 \wedge p_1 \neq p_4 \wedge p_2 \neq p_3 \wedge$   
 $p_2 \neq p_4 \wedge p_3 \neq p_4 \wedge$

$l1 \neq l2 \wedge l1 \neq l3 \wedge l4 \neq l2 \wedge l4 \neq l3 \wedge$   
*(incidente p1 l1  $\wedge$  incidente p2 l1)  $\wedge$*   
*(incidente p1 l2  $\wedge$  incidente p4 l2)  $\wedge$*   
*(incidente p2 l3  $\wedge$  incidente p3 l3)  $\wedge$*   
*(incidente p3 l4  $\wedge$  incidente p4 l4) by (rule laxiomv3)*

**then obtain**  $p1 p2 p3 p4 l1 l2 l3 l4$  **where**

*distintos-p1-p2:  $p1 \neq p2$  and distintos-p1-p3:  $p1 \neq p3$  and*  
*distintos-p1-p4:  $p1 \neq p4$  and distintos-p2-p3:  $p2 \neq p3$  and*  
*distintos-p2-p4:  $p2 \neq p4$  and distintos-p3-p4:  $p3 \neq p4$  and*  
*distintas-l1-l2:  $l1 \neq l2$  and distintas-l1-l3:  $l1 \neq l3$  and*  
*distintas-l4-l2:  $l4 \neq l2$  and distintas-l4-l3:  $l4 \neq l3$  and*  
*incidente-p1-l1: incidente p1 l1 and incidente-p2-l1: incidente p2 l1 and*  
*incidente-p1-l2: incidente p1 l2 and incidente-p4-l2: incidente p4 l2 and*  
*incidente-p2-l3: incidente p2 l3 and incidente-p3-l3: incidente p3 l3 and*  
*incidente-p3-l4: incidente p3 l4 and incidente-p4-l4: incidente p4 l4 by auto*

**have** *equivalente:  $\forall l. p1 \neq p2 \wedge p1 \neq p3 \wedge p1 \neq p4 \wedge$*   
 $p2 \neq p3 \wedge p2 \neq p4 \wedge p3 \neq p4 \wedge$   
 $\neg((\text{incidente } p1 l \wedge \text{incidente } p2 l \wedge \text{incidente } p3 l) \vee$   
 $(\text{incidente } p1 l \wedge \text{incidente } p2 l \wedge \text{incidente } p4 l) \vee$   
 $(\text{incidente } p1 l \wedge \text{incidente } p3 l \wedge \text{incidente } p4 l) \vee$   
 $(\text{incidente } p2 l \wedge \text{incidente } p3 l \wedge \text{incidente } p4 l))$

**proof**

**fix**  $l$

**show**  $p1 \neq p2 \wedge p1 \neq p3 \wedge p1 \neq p4 \wedge$   
 $p2 \neq p3 \wedge p2 \neq p4 \wedge p3 \neq p4 \wedge$   
 $\neg((\text{incidente } p1 l \wedge \text{incidente } p2 l \wedge \text{incidente } p3 l) \vee$   
 $(\text{incidente } p1 l \wedge \text{incidente } p2 l \wedge \text{incidente } p4 l) \vee$   
 $(\text{incidente } p1 l \wedge \text{incidente } p3 l \wedge \text{incidente } p4 l) \vee$   
 $(\text{incidente } p2 l \wedge \text{incidente } p3 l \wedge \text{incidente } p4 l))$

**proof** —

**from** *distintos-p1-p2 and distintos-p1-p3 and*

*distintos-p1-p4 and distintos-p2-p3 and*

*distintos-p2-p4 and distintos-p3-p4*

**have**  $p1 \neq p2 \wedge p1 \neq p3 \wedge p1 \neq p4 \wedge$

$p2 \neq p3 \wedge p2 \neq p4 \wedge p3 \neq p4$  **by simp**

**moreover**

**have**  $\neg((\text{incidente } p1 l \wedge \text{incidente } p2 l \wedge \text{incidente } p3 l) \vee$   
 $(\text{incidente } p1 l \wedge \text{incidente } p2 l \wedge \text{incidente } p4 l) \vee$   
 $(\text{incidente } p1 l \wedge \text{incidente } p3 l \wedge \text{incidente } p4 l) \vee$   
 $(\text{incidente } p2 l \wedge \text{incidente } p3 l \wedge \text{incidente } p4 l))$

**proof**

**assume**  $(\text{incidente } p1 l \wedge \text{incidente } p2 l \wedge \text{incidente } p3 l) \vee$   
 $(\text{incidente } p1 l \wedge \text{incidente } p2 l \wedge \text{incidente } p4 l) \vee$

$(\text{incidente } p1 \ l \wedge \text{incidente } p3 \ l \wedge \text{incidente } p4 \ l) \vee$   
 $(\text{incidente } p2 \ l \wedge \text{incidente } p3 \ l \wedge \text{incidente } p4 \ l)$   
**show** *False*  
**proof** (*rule disjE*)  
**assume** *hip-aux: incidente p1 l ∧ incidente p2 l ∧ incidente p3 l*  
**show** *False*  
**proof** –  
**from** *hip-aux* **have** *incidente p1 l ∧ incidente p2 l* **by** *simp*  
**with** *distintos-p1-p2* **and** *incidente-p1-l1* **and** *incidente-p2-l1*  
**have**  $p1 \neq p2 \wedge (\text{incidente } p1 \ l \wedge \text{incidente } p2 \ l) \wedge$   
 $(\text{incidente } p1 \ l1 \wedge \text{incidente } p2 \ l1)$  **by** *simp*  
**hence**  $l=l1$  **by** (*rule mp[OF axiomv1b]*)  
**moreover**  
**from** *hip-aux* **have** *incidente p2 l ∧ incidente p3 l* **by** *simp*  
**with** *distintos-p2-p3* **and** *incidente-p2-l3* **and** *incidente-p3-l3*  
**have**  $p2 \neq p3 \wedge (\text{incidente } p2 \ l \wedge \text{incidente } p3 \ l) \wedge$   
 $(\text{incidente } p2 \ l3 \wedge \text{incidente } p3 \ l3)$  **by** *simp*  
**hence**  $l=l3$  **by** (*rule mp[OF axiomv1b]*)  
**ultimately** **have**  $l1=l3$  **by** *simp*  
**with** *distintas-l1-l3* **show** *False* **by** *simp*  
**qed**  
**next**  
**assume**  $(\text{incidente } p1 \ l \wedge \text{incidente } p2 \ l \wedge \text{incidente } p4 \ l) \vee$   
 $(\text{incidente } p1 \ l \wedge \text{incidente } p3 \ l \wedge \text{incidente } p4 \ l) \vee$   
 $(\text{incidente } p2 \ l \wedge \text{incidente } p3 \ l \wedge \text{incidente } p4 \ l)$   
**show** *False*  
**proof** (*rule disjE*)  
**assume** *hip-aux: incidente p1 l ∧ incidente p2 l ∧ incidente p4 l*  
**show** *False*  
**proof** –  
**from** *hip-aux* **have** *incidente p1 l ∧ incidente p2 l* **by** *simp*  
**with** *distintos-p1-p2* **and** *incidente-p1-l1* **and** *incidente-p2-l1*  
**have**  $p1 \neq p2 \wedge (\text{incidente } p1 \ l \wedge \text{incidente } p2 \ l) \wedge$   
 $(\text{incidente } p1 \ l1 \wedge \text{incidente } p2 \ l1)$  **by** *simp*  
**hence**  $l=l1$  **by** (*rule mp[OF axiomv1b]*)  
**moreover**  
**from** *hip-aux* **have** *incidente p1 l ∧ incidente p4 l* **by** *simp*  
**with** *distintos-p1-p4* **and** *incidente-p1-l2* **and** *incidente-p4-l2*  
**have**  $p1 \neq p4 \wedge (\text{incidente } p1 \ l \wedge \text{incidente } p4 \ l) \wedge$   
 $(\text{incidente } p1 \ l2 \wedge \text{incidente } p4 \ l2)$  **by** *simp*  
**hence**  $l=l2$  **by** (*rule mp[OF axiomv1b]*)  
**ultimately**  
**have**  $l1=l2$  **by** *simp*

**with** *distintas-l1-l2* **show** *False* **by** *simp*  
**qed**  
**next**  
**assume** (*incidente p1 l*  $\wedge$  *incidente p3 l*  $\wedge$  *incidente p4 l*)  $\vee$   
     (*incidente p2 l*  $\wedge$  *incidente p3 l*  $\wedge$  *incidente p4 l*)  
**show** *False*  
**proof** (*rule disjE*)  
**assume** *hip-aux: incidente p1 l*  $\wedge$  *incidente p3 l*  $\wedge$  *incidente p4 l*  
**show** *False*  
**proof** –  
**from** *hip-aux* **have** *incidente p1 l*  $\wedge$  *incidente p4 l* **by** *simp*  
**with** *distintos-p1-p4* **and** *incidente-p1-l2* **and** *incidente-p4-l2*  
**have**  $p1 \neq p4 \wedge$  (*incidente p1 l*  $\wedge$  *incidente p4 l*)  $\wedge$   
     (*incidente p1 l2*  $\wedge$  *incidente p4 l2*) **by** *simp*  
**hence**  $l=l2$  **by** (*rule mp[OF axiomv1b]*)  
**moreover**  
**from** *hip-aux* **have** *incidente p3 l*  $\wedge$  *incidente p4 l* **by** *simp*  
**with** *distintos-p3-p4* **and** *incidente-p3-l4* **and** *incidente-p4-l4*  
**have**  $p3 \neq p4 \wedge$  (*incidente p3 l*  $\wedge$  *incidente p4 l*)  $\wedge$   
     (*incidente p3 l4*  $\wedge$  *incidente p4 l4*) **by** *simp*  
**hence**  $l=l4$  **by** (*rule mp[OF axiomv1b]*)  
**ultimately**  
**have**  $l2=l4$  **by** *simp*  
**with** *distintas-l4-l2* **show** *False* **by** *simp*  
**qed**  
**next**  
**assume** *hip-aux: incidente p2 l*  $\wedge$  *incidente p3 l*  $\wedge$  *incidente p4 l*  
**show** *False*  
**proof** –  
**from** *hip-aux* **have** *incidente p2 l*  $\wedge$  *incidente p3 l* **by** *simp*  
**with** *distintos-p2-p3* **and** *incidente-p2-l3* **and** *incidente-p3-l3*  
**have**  $p2 \neq p3 \wedge$  (*incidente p2 l*  $\wedge$  *incidente p3 l*)  $\wedge$   
     (*incidente p2 l3*  $\wedge$  *incidente p3 l3*) **by** *simp*  
**hence**  $l=l3$  **by** (*rule mp[OF axiomv1b]*)  
**moreover**  
**from** *hip-aux* **have** *incidente p3 l*  $\wedge$  *incidente p4 l* **by** *simp*  
**with** *distintos-p3-p4* **and** *incidente-p3-l4* **and** *incidente-p4-l4*  
**have**  $p3 \neq p4 \wedge$  (*incidente p3 l*  $\wedge$  *incidente p4 l*)  $\wedge$   
     (*incidente p3 l4*  $\wedge$  *incidente p4 l4*) **by** *simp*  
**hence**  $l=l4$  **by** (*rule mp[OF axiomv1b]*)  
**ultimately**  
**have**  $l3=l4$  **by** *simp*  
**with** *distintas-l4-l3* **show** *False* **by** *simp*

```

      qed
    qed
  qed
  qed
  qed
  ultimately
  show ?thesis by simp
  qed
  qed
  have (∀ l. p1≠p2 ∧ p1≠p3 ∧ p1≠p4 ∧
    p2≠p3 ∧ p2≠p4 ∧ p3≠p4 ∧
    ¬((incidente p1 l ∧ incidente p2 l ∧ incidente p3 l) ∨
    (incidente p1 l ∧ incidente p2 l ∧ incidente p4 l) ∨
    (incidente p1 l ∧ incidente p3 l ∧ incidente p4 l) ∨
    (incidente p2 l ∧ incidente p3 l ∧ incidente p4 l))) ≡
    (∀ l. p1≠p2 ∧ p1≠p3 ∧ p1≠p4 ∧
    p2≠p3 ∧ p2≠p4 ∧ p3≠p4 ∧
    ¬(incidente p1 l ∧ incidente p2 l ∧ incidente p3 l) ∧
    ¬(incidente p1 l ∧ incidente p2 l ∧ incidente p4 l) ∧
    ¬(incidente p1 l ∧ incidente p3 l ∧ incidente p4 l) ∧
    ¬(incidente p2 l ∧ incidente p3 l ∧ incidente p4 l)) by simp
  with equivalente have ∀ l. p1≠p2 ∧ p1≠p3 ∧ p1≠p4 ∧
    p2≠p3 ∧ p2≠p4 ∧ p3≠p4 ∧
    ¬(incidente p1 l ∧ incidente p2 l ∧ incidente p3 l) ∧
    ¬(incidente p1 l ∧ incidente p2 l ∧ incidente p4 l) ∧
    ¬(incidente p1 l ∧ incidente p3 l ∧ incidente p4 l) ∧
    ¬(incidente p2 l ∧ incidente p3 l ∧ incidente p4 l) by simp
  thus ?thesis by auto
  qed

```

## 9.4 Algunas nociones básicas de la geometría proyectiva

En esta parte formalizamos en Isar algunas definiciones que aparecen en el estudio de la geometría proyectiva.

**Definición 9.4.1** *Un punto está en la intersección de dos rectas si es un punto incidente con ambas rectas.*

```

consts interseccion :: punto ⇒ recta ⇒ recta ⇒ bool
defs
interseccion-def:

```



$interseccion\ p\ x\ y \equiv (incidente\ p\ x \wedge incidente\ p\ y)$

En la definición anterior las rectas  $x$  y  $y$  pueden ser iguales, en este caso el punto de intersección no es único.

**Definición 9.4.2** Una recta está en la conexión de dos puntos si la recta incidente con ambos puntos.

**consts**  $conexion :: recta \Rightarrow punto \Rightarrow punto \Rightarrow bool$

**defs**

$conexion-def:$

$conexion\ l\ x\ y \equiv (incidente\ x\ l \wedge incidente\ y\ l)$

En la definición anterior los puntos  $x$  y  $y$  pueden ser iguales, en este caso la recta de conexión no es única.

**Definición 9.4.3** Los puntos  $A_i (i = 1, \dots, n)$  son colineales si existe una recta con la que todos los puntos son incidentes.

**consts**  $colineales :: punto\ set \Rightarrow bool$

**defs**

$colineales-def:$

$colineales\ A \equiv (\exists\ l. \forall\ p \in A. incidente\ p\ l)$

**Definición 9.4.4** Las rectas  $l_i (i = 1, \dots, n)$  son concurrentes si existe un punto con el que todas las rectas son incidentes.

**consts**  $concurrentes :: recta\ set \Rightarrow bool$

**defs**

$concurrentes-def:$

$concurrentes\ A \equiv (\exists\ p. \forall\ l \in A. incidente\ p\ l)$

**Definición 9.4.5** Un triángulo es un conjunto de tres puntos distintos  $A_1, A_2, A_3$  y tres rectas  $a_1, a_2, a_3$  tal que  $A_i$  es incidente con  $a_k$  para  $i \neq k$  y  $A_i$  no es incidente con  $a_i$  ( $i, k = 1, 2, 3$ ). Los puntos  $A_i$  son los vértices y las rectas  $a_i$  los lados del triángulo.  $A_i$  es el vértice opuesto al lado  $a_i$ . Usamos la notación  $(triangulo\ A_1\ A_2\ A_3\ a_1\ a_2\ a_3)$  para referirnos al triángulo definido anteriormente.

```

consts triangulo :: punto  $\Rightarrow$  punto  $\Rightarrow$  punto  $\Rightarrow$ 
                recta  $\Rightarrow$  recta  $\Rightarrow$  recta  $\Rightarrow$  bool

```

**defs**

*triangulo-def:*

```

triangulo A1 A2 A3 a1 a2 a3  $\equiv$ 
((A1  $\neq$  A2  $\wedge$  A1  $\neq$  A3  $\wedge$  A2  $\neq$  A3)  $\wedge$ 
 (incidente A1 a2  $\wedge$  incidente A1 a3)  $\wedge$ 
 (incidente A2 a1  $\wedge$  incidente A2 a3)  $\wedge$ 
 (incidente A3 a1  $\wedge$  incidente A3 a2)  $\wedge$ 
 ( $\neg$ incidente A1 a1  $\wedge$   $\neg$ incidente A2 a2  $\wedge$   $\neg$ incidente A3 a3))

```

## 9.5 Algunas consecuencias de las definiciones

Los siguientes dos resultados afirman que si una recta conecta dos puntos, entonces es incidente con ellos.

**theorem**

**assumes** *conexion* l x y

**shows** *incidente* x l

**proof** –

**show** *incidente* x l **using** *assms* **by** (*simp add: conexion-def*)

**qed**

**theorem**

**assumes** *conexion* l x y

**shows** *incidente* y l

**proof** –

**show** *incidente* y l **using** *assms* **by** (*simp add: conexion-def*)

**qed**

Los resultados duales a los anteriores, afirman que si un punto está en la intersección de dos rectas, entonces es incidente con ellas.

**theorem**

**assumes** *interseccion* p x y

**shows** *incidente* p x

**proof** –

**show** *incidente* p x **using** *assms* **by** (*simp add: interseccion-def*)

**qed**

**theorem**

**assumes** *interseccion* p x y

**shows** *incidente* p y

**proof** –

**show** *incidente p* **using** *assms* **by** (*simp add: interseccion-def*)  
**qed**

La existencia de un punto de intersección de dos rectas cualesquiera está garantizada por el siguiente teorema.

**theorem** *existencia-interseccion*:  $\exists p. \text{interseccion } p \ l1 \ l2$

**proof** –

**have** *casos*:  $l1 = l2 \vee l1 \neq l2$  **by** *simp*

**from** *casos* **show** *?thesis*

**proof** *cases*

**assume**  $l1=l2$

**moreover**

**from** *axiomv4* **have**  $\exists p. \text{incidente } p \ l1$  **by** *auto*

**then obtain**  $p$  **where** *incidente-p-l1*:  $\text{incidente } p \ l1$  **by** (*rule exE*)

**ultimately**

**have** *incidente-p-l2*:  $\text{incidente } p \ l2$  **by** *simp*

**with** *incidente-p-l1* **have**  $\text{interseccion } p \ l1 \ l2$  **by** (*simp add: interseccion-def*)

**thus** *?thesis* **by** *auto*

**next**

**assume**  $l1 \neq l2$

**have**  $\exists p. \text{incidente } p \ l1 \wedge \text{incidente } p \ l2$  **by** (*rule mp[OF axiomv2]*)

**thus** *?thesis* **by** (*simp add: interseccion-def*)

**qed**

**qed**

El teorema dual de la proposición anterior afirma la existencia de una recta de conexión de dos puntos cualesquiera.

**theorem** *existencia-conexion*:  $\exists l. \text{conexion } l \ p1 \ p2$

**proof** –

**have** *casos*:  $p1 = p2 \vee p1 \neq p2$  **by** *simp*

**from** *casos* **show** *?thesis*

**proof** *cases*

**assume**  $p1=p2$

**moreover**

**from** *DV4* **have**  $\exists l. \text{incidente } p1 \ l$  **by** *auto*

**then obtain**  $l$  **where** *incidente-p1-l*:  $\text{incidente } p1 \ l$  **by** (*rule exE*)

**ultimately**

**have** *incidente-p2-l*:  $\text{incidente } p2 \ l$  **by** *simp*

**with** *incidente-p1-l* **have**  $\text{conexion } l \ p1 \ p2$  **by** (*simp add: conexion-def*)

**thus** *?thesis* **by** *auto*

**next**

**assume**  $p1 \neq p2$

**have**  $\exists l. \text{incidente } p1 \ l \wedge \text{incidente } p2 \ l$  **by** (*rule mp[OF axiomv1a]*)

**thus ?thesis by** (*simp add: conexion-def*)  
**qed**  
**qed**

Usando el concepto de rectas concurrentes para el caso particular de tres rectas, se tiene que si un punto es incidente con tres rectas, las tres rectas son concurrentes.

**theorem concurrentes-tres:**

**assumes** *incidente p c1*

**and** *incidente p c2*

**and** *incidente p c3*

**shows** *concurrentes{c1,c2,c3}*

**proof** –

**have**  $\forall l \in \{c1, c2, c3\}. \textit{incidente } p \ l$  **using** *assms by simp*

**hence**  $\exists p. \forall l \in \{c1, c2, c3\}. \textit{incidente } p \ l$  **by** (*rule ex1*)

**thus ?thesis by** (*simp add: concurrentes-def*)

**qed**

El siguiente teorema formaliza en qué casos un conjunto de tres puntos y tres rectas no forman un triángulo.

**theorem no-triangulo:**

$\neg (\textit{triangulo } A1 \ A2 \ A3 \ a1 \ a2 \ a3) \equiv$

$(A1 = A2 \vee A1 = A3 \vee A2 = A3) \vee$

$\neg(\textit{incidente } A1 \ a2) \vee \neg(\textit{incidente } A1 \ a3) \vee$

$\neg(\textit{incidente } A2 \ a1) \vee \neg(\textit{incidente } A2 \ a3) \vee$

$\neg(\textit{incidente } A3 \ a1) \vee \neg(\textit{incidente } A3 \ a2) \vee$

$(\textit{incidente } A1 \ a1 \vee \textit{incidente } A2 \ a2 \vee \textit{incidente } A3 \ a3)$

**proof** –

**have**

*equivalente1:*  $\neg (\textit{triangulo } A1 \ A2 \ A3 \ a1 \ a2 \ a3) \equiv$

$\neg((A1 \neq A2 \wedge A1 \neq A3 \wedge A2 \neq A3) \wedge$

$((\textit{incidente } A1 \ a2 \wedge \textit{incidente } A1 \ a3) \wedge$

$(\textit{incidente } A2 \ a1 \wedge \textit{incidente } A2 \ a3) \wedge$

$(\textit{incidente } A3 \ a1 \wedge \textit{incidente } A3 \ a2))) \wedge$

$(\neg \textit{incidente } A1 \ a1 \wedge \neg \textit{incidente } A2 \ a2 \wedge \neg \textit{incidente } A3 \ a3))$

**by**(*simp add: triangulo-def*)

**have**

*equivalente2:*  $\neg((A1 \neq A2 \wedge A1 \neq A3 \wedge A2 \neq A3) \wedge$

$((\textit{incidente } A1 \ a2 \wedge \textit{incidente } A1 \ a3) \wedge$

$(\textit{incidente } A2 \ a1 \wedge \textit{incidente } A2 \ a3) \wedge$

$(\textit{incidente } A3 \ a1 \wedge \textit{incidente } A3 \ a2))) \wedge$

$(\neg \textit{incidente } A1 \ a1 \wedge \neg \textit{incidente } A2 \ a2 \wedge \neg \textit{incidente } A3 \ a3)) \equiv$

$(A1 = A2 \vee A1 = A3 \vee A2 = A3) \vee$

$\neg(\textit{incidente } A1 \ a2) \vee \neg(\textit{incidente } A1 \ a3) \vee$

$$\begin{aligned} & \neg(\text{incidente } A2 \ a1) \vee \neg(\text{incidente } A2 \ a3) \vee \\ & \neg(\text{incidente } A3 \ a1) \vee \neg(\text{incidente } A3 \ a2) \vee \\ & (\text{incidente } A1 \ a1 \vee \text{incidente } A2 \ a2 \vee \text{incidente } A3 \ a3) \\ & \text{by simp} \end{aligned}$$

**from** *equivalente1* and *equivalente2*

**show**

$$\begin{aligned} & \neg(\text{triangulo } A1 \ A2 \ A3 \ a1 \ a2 \ a3) \equiv \\ & (A1 = A2 \vee A1 = A3 \vee A2 = A3) \vee \\ & \neg(\text{incidente } A1 \ a2) \vee \neg(\text{incidente } A1 \ a3) \vee \\ & \neg(\text{incidente } A2 \ a1) \vee \neg(\text{incidente } A2 \ a3) \vee \\ & \neg(\text{incidente } A3 \ a1) \vee \neg(\text{incidente } A3 \ a2) \vee \\ & (\text{incidente } A1 \ a1 \vee \text{incidente } A2 \ a2 \vee \text{incidente } A3 \ a3) \text{ by simp} \end{aligned}$$

qed

## 9.6 Proposición de Desargues

**Axioma (axiomdesargues)** Consideremos los triángulos  $A_1A_2A_3a_1a_2a_3$  y  $B_1B_2B_3b_1b_2b_3$ , con vértices  $A_i$  y  $B_i$ , y lados opuestos  $a_i$  y  $b_i$  respectivamente ( $i = 1, 2, 3$ ). Supongamos que para  $i = 1, 2, 3$  se tiene que  $A_i \neq B_i$  y  $a_i \neq b_i$ , además sea  $c_i$  la recta que une los puntos  $A_i, B_i$  y  $C_i$  el punto de intersección de las rectas  $a_i, b_i$ . Entonces, si las rectas  $c_i$  son concurrentes, los puntos  $C_i$  son colineales (ver Figura 9.8).

**axioms**

*axiomdesargues:*

$$\begin{aligned} & \llbracket \text{triangulo } A1 \ A2 \ A3 \ a1 \ a2 \ a3; \\ & \text{triangulo } B1 \ B2 \ B3 \ b1 \ b2 \ b3; \\ & A1 \neq B1; A2 \neq B2; A3 \neq B3; \\ & a1 \neq b1; a2 \neq b2; a3 \neq b3; \\ & \text{conexion } c1 \ A1 \ B1; \text{conexion } c2 \ A2 \ B2; \text{conexion } c3 \ A3 \ B3; \\ & \text{concurrentes } \{c1, c2, c3\} \rrbracket \implies \\ & (\text{interseccion } C1 \ a1 \ b1) \wedge (\text{interseccion } C2 \ a2 \ b2) \wedge \\ & (\text{interseccion } C3 \ a3 \ b3) \wedge \text{colineales } \{C1, C2, C3\} \end{aligned}$$

Otra forma de enunciar el axioma anterior es reemplazando los predicados conexión, concurrentes, intersección y colineales por sus correspondientes definiciones (ver Figura 9.8).

**lemma** *desargues1a:*

**assumes** *triangulos:*  $\text{triangulo } A1 \ A2 \ A3 \ a1 \ a2 \ a3 \wedge \text{triangulo } B1 \ B2 \ B3 \ b1 \ b2 \ b3$

**and** *vertices-diferentes:*  $A1 \neq B1 \wedge A2 \neq B2 \wedge A3 \neq B3$

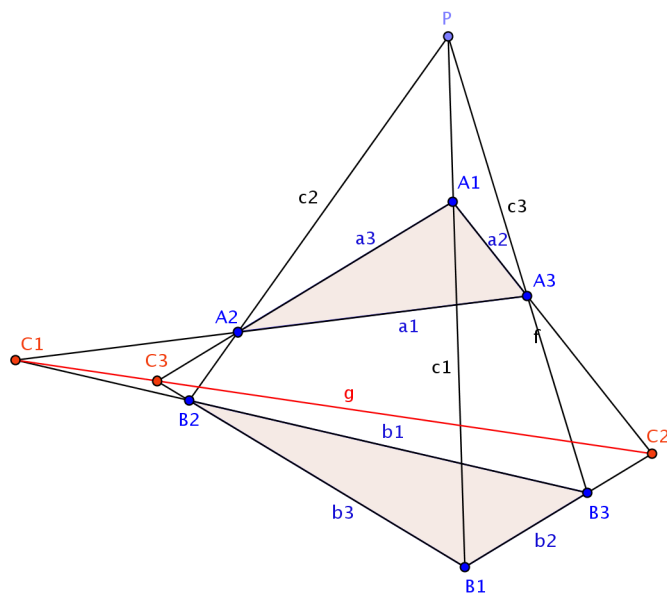


Figura 9.8: Axioma de Desargues

**and** *lados-diferentes*:  $a1 \neq b1 \wedge a2 \neq b2 \wedge a3 \neq b3$   
**and** *incidente-A1-c1*: *incidente A1 c1*  
**and** *incidente-A2-c2*: *incidente A2 c2*  
**and** *incidente-A3-c3*: *incidente A3 c3*  
**and** *incidente-B1-c1*: *incidente B1 c1*  
**and** *incidente-B2-c2*: *incidente B2 c2*  
**and** *incidente-B3-c3*: *incidente B3 c3*  
**and** *incidente-P-c1*: *incidente P c1*  
**and** *incidente-P-c2*: *incidente P c2*  
**and** *incidente-P-c3*: *incidente P c3*  
**shows**  $\exists C1 C2 C3 l$ .  
*incidente C1 a1*  $\wedge$  *incidente C1 b1*  $\wedge$  *incidente C1 l*  $\wedge$   
*incidente C2 a2*  $\wedge$  *incidente C2 b2*  $\wedge$  *incidente C2 l*  $\wedge$   
*incidente C3 a3*  $\wedge$  *incidente C3 b3*  $\wedge$  *incidente C3 l*  
**proof** –  
**have** *lados-diferentes*:  $a1 \neq b1 \wedge a2 \neq b2 \wedge a3 \neq b3$ .  
**moreover**  
**from** *incidente-A1-c1* **and** *incidente-B1-c1*  
**have** *conexion c1 A1 B1* **by** (*simp add: conexion-def*)  
**moreover**  
**from** *incidente-A2-c2* **and** *incidente-B2-c2*  
**have** *conexion c2 A2 B2* **by** (*simp add: conexion-def*)  
**moreover**  
**from** *incidente-A3-c3* **and** *incidente-B3-c3*  
**have** *conexion c3 A3 B3* **by** (*simp add: conexion-def*)  
**moreover**  
**from** *incidente-P-c1* **and** *incidente-P-c2* **and** *incidente-P-c3*  
**have** *concurrentes*  $\{c1, c2, c3\}$  **by** (*rule concurrentes-tres*)  
**moreover**  
**from** *triangulos*  
**have** *triangulo A1 A2 A3 a1 a2 a3* **by** *simp*  
**moreover**  
**from** *triangulos*  
**have** *triangulo B1 B2 B3 b1 b2 b3* **by** *simp*  
**moreover**  
**from** *vertices-diferentes*  
**have**  $A1 \neq B1 \wedge A2 \neq B2 \wedge A3 \neq B3$  **by** *simp*  
**ultimately**  
**have** *conclusion*:  $(\text{interseccion } C1 \ a1 \ b1) \wedge (\text{interseccion } C2 \ a2 \ b2) \wedge$   
 $(\text{interseccion } C3 \ a3 \ b3) \wedge \text{colineales } \{C1, C2, C3\}$   
**by** (*simp add: axiomdesargues*)  
**from** *conclusion*  
**have** *incidente C1 a1*  $\wedge$  *incidente C1 b1*  $\wedge$

*incidente C2 a2*  $\wedge$  *incidente C2 b2*  $\wedge$   
*incidente C3 a3*  $\wedge$  *incidente C3 b3* **by** (*simp add: interseccion-def*)  
**moreover**  
**from** *conclusion*  
**have**  $\exists l. \forall p \in \{C1, C2, C3\}. \textit{incidente } p \ l$   
**by** (*simp add: colineales-def*)  
**then obtain l where**  
*incidente C1 l*  $\wedge$  *incidente C2 l*  $\wedge$  *incidente C3 l* **by** *auto*  
**ultimately show ?thesis** **by** *auto*  
**qed**

Los siguientes lemas establecen condiciones suficientes para la conclusión del axioma de Desargues.

**Lema 9.6.1 (desargues1b)** Sean  $a_i, b_i$  ( $i = 1, 2, 3$ ) rectas tales que,  $\neg(a_1 \neq b_1 \wedge a_2 \neq b_2 \wedge a_3 \neq b_3)$ . Entonces, existen tres puntos  $C_1, C_2, C_3$  y una recta  $l$  tales que  $C_1$  es incidente con  $a_1, b_1, l$ ;  $C_2$  es incidente con  $a_2, b_2, l$ ;  $C_3$  es incidente con  $a_3, b_3, l$ .

**Demostración:** Supongamos que  $\neg(a_1 \neq b_1 \wedge a_2 \neq b_2 \wedge a_3 \neq b_3)$ , entonces  $a_1 = b_1 \vee a_2 = b_2 \vee a_3 = b_3$ . De esto último, hacemos la demostración por casos. Supongamos  $a_1 = b_1$ . Sea  $C_2$  el punto de intersección de  $a_2$  y  $b_2$ ;  $C_3$  el punto de intersección de  $a_3$  y  $b_3$ ;  $l$  la recta de conexión de  $C_2$  y  $C_3$ . Entonces,  $C_2$  es incidente con  $a_2, b_2, l$  y  $C_3$  es incidente con  $a_3, b_3, l$ . Sea  $C_1$  el punto de intersección de  $a_1$  y  $l$ , entonces  $C_1$  es incidente con  $a_1 = b_1$  y  $l$ . De esta forma, en este caso, queda demostrado el lema (ver Figura 9.9).

En los casos  $a_2 = b_2$  o  $a_3 = b_3$ , las demostraciones son análogas a la anterior. □

**lemma** *desargues1b*:

**assumes**  $\neg(a_1 \neq b_1 \wedge a_2 \neq b_2 \wedge a_3 \neq b_3)$

**shows**  $\exists C1 \ C2 \ C3 \ l.$

*incidente C1 a1*  $\wedge$  *incidente C1 b1*  $\wedge$  *incidente C1 l*  $\wedge$

*incidente C2 a2*  $\wedge$  *incidente C2 b2*  $\wedge$  *incidente C2 l*  $\wedge$

*incidente C3 a3*  $\wedge$  *incidente C3 b3*  $\wedge$  *incidente C3 l*

**proof** –

**from** *assms* **have**  $a_1 = b_1 \vee a_2 = b_2 \vee a_3 = b_3$  **by** *simp*

**thus** *?thesis*

**proof** (*rule disjE*)

**assume** *hip-aux*:  $a_1 = b_1$

**show** *?thesis*

**proof** –

**have**  $\exists C2. \textit{interseccion } C2 \ a2 \ b2$  **by** (*rule existencia-interseccion*)

**then obtain C2 where** *incidente C2 a2*  $\wedge$  *incidente C2 b2*

**by** (*simp add: interseccion-def*) *auto*



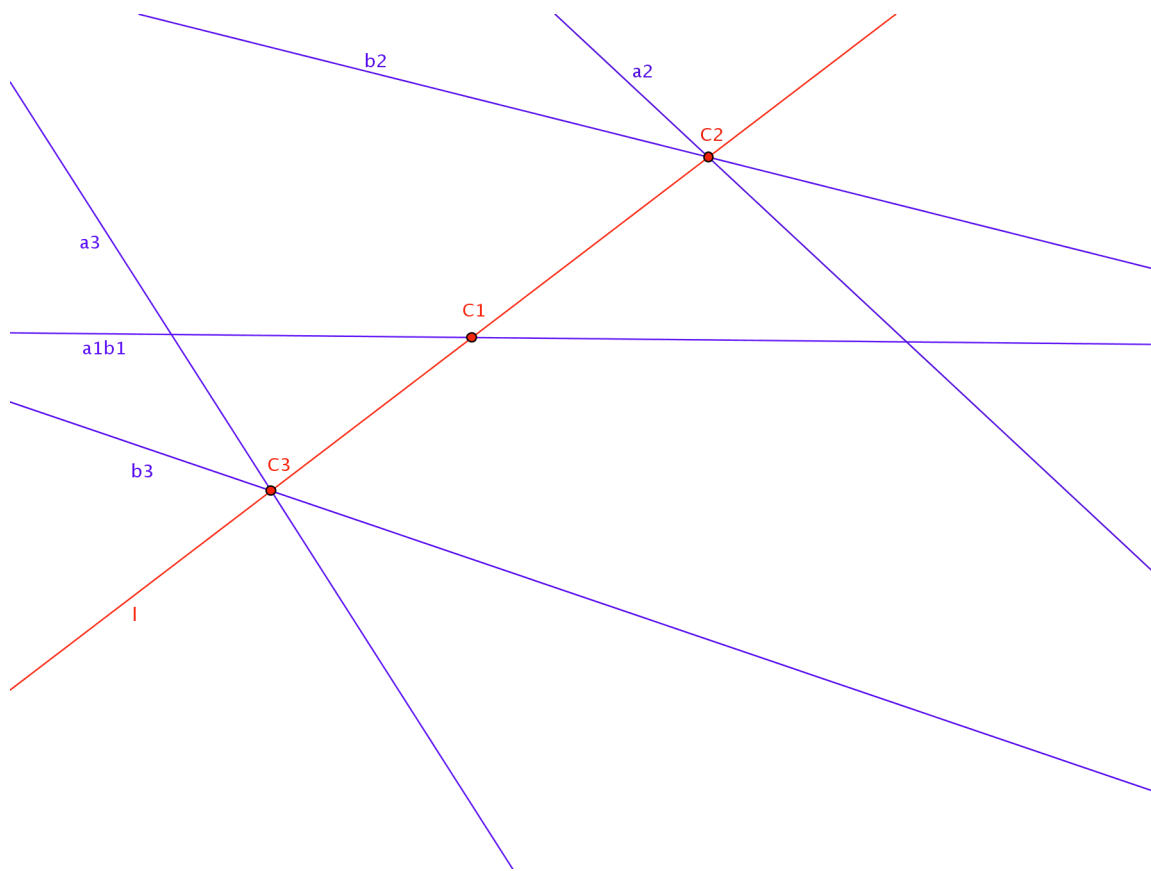


Figura 9.9: Lema 9.6.1

**moreover**  
**have**  $\exists C3$ . *interseccion* C3 a3 b3 **by** (*rule existencia-interseccion*)  
**then obtain** C3 **where** *incidente* C3 a3  $\wedge$  *incidente* C3 b3  
**by** (*simp add: interseccion-def*) *auto*  
**moreover**  
**have**  $\exists l$ . *conexion* l C2 C3 **by** (*simp add: existencia-conexion*)  
**then obtain** l **where** *incidente* C2 l  $\wedge$  *incidente* C3 l  
**by**(*simp add: conexion-def*) *auto*  
**moreover**  
**have**  $\exists C1$ . *interseccion* C1 a1 l **by** (*rule existencia-interseccion*)  
**then obtain** C1 **where** *incidente* C1 a1  $\wedge$  *incidente* C1 l  
**by** (*simp add: interseccion-def*) *auto*  
**moreover**  
**with** *hip-aux* **have** *incidente* C1 b1 **by** *simp*  
**ultimately**  
**show** ?thesis **by** *auto*  
**qed**  
**next**  
**assume**  $a2 = b2 \vee a3 = b3$   
**show** ?thesis  
**proof** (*rule disjE*)  
**assume** *hip-aux*:  $a2=b2$   
**show** ?thesis  
**proof** –  
**have**  $\exists C1$ . *interseccion* C1 a1 b1 **by** (*rule existencia-interseccion*)  
**then obtain** C1 **where** *incidente* C1 a1  $\wedge$  *incidente* C1 b1  
**by** (*simp add: interseccion-def*) *auto*  
**moreover**  
**have**  $\exists C3$ . *interseccion* C3 a3 b3 **by** (*rule existencia-interseccion*)  
**then obtain** C3 **where** *incidente* C3 a3  $\wedge$  *incidente* C3 b3  
**by** (*simp add: interseccion-def*) *auto*  
**moreover**  
**have**  $\exists l$ . *conexion* l C1 C3 **by** (*simp add: existencia-conexion*)  
**then obtain** l **where** *incidente* C1 l  $\wedge$  *incidente* C3 l  
**by**(*simp add: conexion-def*) *auto*  
**moreover**  
**have**  $\exists C2$ . *interseccion* C2 a2 l **by** (*rule existencia-interseccion*)  
**then obtain** C2 **where** *incidente* C2 a2  $\wedge$  *incidente* C2 l  
**by** (*simp add: interseccion-def*) *auto*  
**moreover**  
**with** *hip-aux* **have** *incidente* C2 b2 **by** *simp*  
**ultimately**  
**show** ?thesis **by** *auto*

```

qed
next
assume hip-aux: a3=b3
show ?thesis
proof –
  have  $\exists C1. \text{interseccion } C1 \ a1 \ b1$  by (rule existencia-interseccion)
  then obtain C1 where incidente C1 a1  $\wedge$  incidente C1 b1
    by (simp add: interseccion-def) auto

  moreover
  have  $\exists C2. \text{interseccion } C2 \ a2 \ b2$  by (rule existencia-interseccion)
  then obtain C2 where incidente C2 a2  $\wedge$  incidente C2 b2
    by (simp add: interseccion-def) auto

  moreover
  have  $\exists l. \text{conexion } l \ C1 \ C2$  by (simp add: existencia-conexion)
  then obtain l where incidente C1 l  $\wedge$  incidente C2 l
    by (simp add: conexion-def) auto

  moreover
  have  $\exists C3. \text{interseccion } C3 \ a3 \ l$  by (rule existencia-interseccion)
  then obtain C3 where incidente C3 a3  $\wedge$  incidente C3 l
    by (simp add: interseccion-def) auto

  moreover
  with hip-aux have incidente C3 b3 by simp
  ultimately
  show ?thesis by auto
qed
qed
qed
qed

```

**Lema 9.6.2 (desargues1c)** Sean  $A_i, B_i$  y  $a_i, b_i$  ( $i = 1, 2, 3$ ) puntos y rectas respectivamente. Supongamos que  $\neg(A_1 \neq B_1 \wedge A_2 \neq B_2 \wedge A_3 \neq B_3)$ ;  $A_1$  es incidente con  $a_2, a_3$ ;  $A_2$  es incidente con  $a_3, a_1$ ;  $A_3$  es incidente con  $a_1, a_2$ ;  $B_1$  es incidente con  $b_2, b_3$ ;  $B_2$  es incidente con  $b_3, b_1$ ;  $B_3$  es incidente con  $b_1, b_2$ . Entonces, existen tres puntos  $C_1, C_2, C_3$  y una recta  $l$  tales que  $C_1$  es incidente con  $a_1, b_1, l$ ;  $C_2$  es incidente con  $a_2, b_2, l$ ;  $C_3$  es incidente con  $a_3, b_3, l$ .

**Demostración:** Supongamos  $\neg(A_1 \neq B_1 \wedge A_2 \neq B_2 \wedge A_3 \neq B_3)$ , entonces  $A_1 = B_1 \vee A_2 = B_2 \vee A_3 = B_3$ . De esto último, se obtiene el resultado por casos. Supongamos que  $A_1 = B_1$ . Sea  $C_1$  el punto de intersección de las rectas  $a_1$  y  $b_1$ , entonces  $C_1$  es incidente con  $a_1, b_1$ . Ahora, sea  $l$  la recta de conexión de  $C_1$  y  $A_1$ , entonces  $C_1, A_1$  son incidentes con  $l$ . Además, usando las hipótesis,  $A_1 = B_1$ ;  $A_1$  incidente con  $a_2, a_3$ ;  $B_1$  incidente con  $b_2, b_3$ , obtenemos que, en total,  $A_1$  es incidente con  $a_2, a_3, b_2, b_3, l$ . Luego, haciendo  $C_2 = C_3 = A_1$ , se tiene en este caso la demostración del lema (ver Figura 9.10).

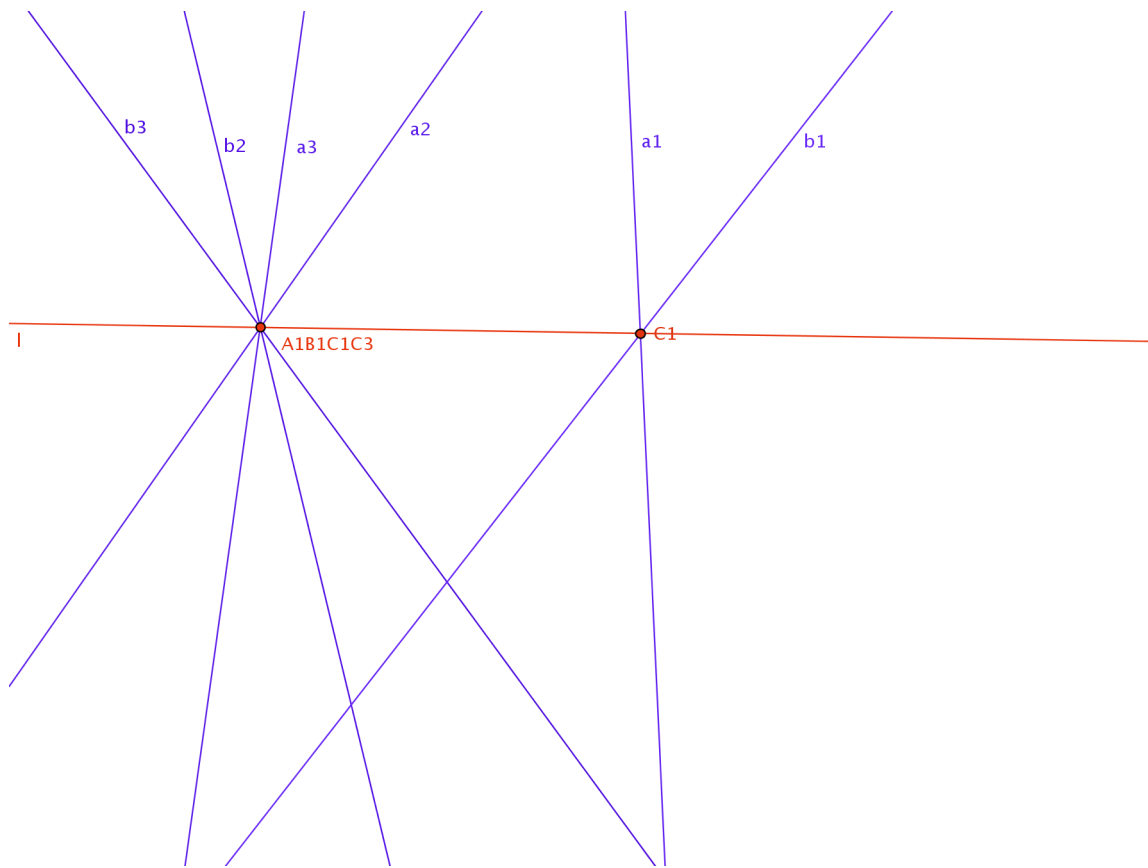


Figura 9.10: Lema 9.6.2

En los casos  $A_2 = B_2$  o  $A_3 = B_3$ , las demostraciones son análogas a la anterior.

□

**lemma** *desargues1c:assumes*

*no-vertices-diferentes*:  $\neg(A_1 \neq B_1 \wedge A_2 \neq B_2 \wedge A_3 \neq B_3)$  **and**

*incidente-A1-a2*: *incidente*  $A_1 a_2$  **and** *incidente-A1-a3*: *incidente*  $A_1 a_3$  **and**

*incidente-A2-a3*: *incidente*  $A_2 a_3$  **and** *incidente-A2-a1*: *incidente*  $A_2 a_1$  **and**

*incidente-A3-a1*: *incidente*  $A_3 a_1$  **and** *incidente-A3-a2*: *incidente*  $A_3 a_2$  **and**

*incidente-B1-b2*: *incidente*  $B_1 b_2$  **and** *incidente-B1-b3*: *incidente*  $B_1 b_3$  **and**

*incidente-B2-b3*: *incidente*  $B_2 b_3$  **and** *incidente-B2-b1*: *incidente*  $B_2 b_1$  **and**

*incidente-B3-b1*: *incidente*  $B_3 b_1$  **and** *incidente-B3-b2*: *incidente*  $B_3 b_2$

**shows**

$\exists C_1 C_2 C_3 l.$

*incidente*  $C_1 a_1 \wedge$  *incidente*  $C_1 b_1 \wedge$  *incidente*  $C_1 l \wedge$

*incidente*  $C_2 a_2 \wedge$  *incidente*  $C_2 b_2 \wedge$  *incidente*  $C_2 l \wedge$

*incidente*  $C_3 a_3 \wedge$  *incidente*  $C_3 b_3 \wedge$  *incidente*  $C_3 l$

**proof** –

**from** *no-vertices-diferentes*

**have** *equivalente*:  $A_1 = B_1 \vee A_2 = B_2 \vee A_3 = B_3$  **by** *simp*

**thus** *?thesis*

**proof** (*rule disjE*)

**assume** *hip-aux*:  $A_1 = B_1$

**show** *?thesis*

**proof** –

**have**  $\exists C_1.$  *interseccion*  $C_1 a_1 b_1$  **by** (*rule existencia-interseccion*)

**then obtain**  $C_1$  **where** *incidente*  $C_1 a_1 \wedge$  *incidente*  $C_1 b_1$

**by** (*simp add: interseccion-def*) *auto*

**moreover**

**have**  $\exists l.$  *conexion*  $l C_1 A_1$  **by** (*simp add: existencia-conexion*)

**then obtain**  $l$  **where** *incidente*  $C_1 l \wedge$  *incidente*  $A_1 l$

**by** (*simp add: conexion-def*) *auto*

**moreover**

**let**  $?C_2 = A_1$

**from** *hip-aux* **and** *incidente-A1-a2* **and** *incidente-B1-b2*

**have** *incidente*  $?C_2 a_2 \wedge$  *incidente*  $?C_2 b_2$  **by** *simp*

**moreover**

**let**  $?C_3 = A_1$

**from** *hip-aux* **and** *incidente-A1-a3* **and** *incidente-B1-b3*

**have** *incidente*  $?C_3 a_3 \wedge$  *incidente*  $?C_3 b_3$  **by** *simp*

**ultimately**

**show** *?thesis* **by** *auto*

**qed**

**next**

**assume**  $A_2 = B_2 \vee A_3 = B_3$

**show** ?thesis  
**proof**(rule disjE)  
**assume** hip-aux: A2=B2  
**show** ?thesis  
**proof** –  
**have**  $\exists C2$ . interseccion C2 a2 b2 **by** (rule existencia-interseccion)  
**then obtain** C2 **where** incidente C2 a2  $\wedge$  incidente C2 b2  
**by** (simp add: interseccion-def) auto  
**moreover**  
**have**  $\exists l$ . conexion l C2 A2 **by** (simp add: existencia-conexion)  
**then obtain** l **where** incidente C2 l  $\wedge$  incidente A2 l  
**by** (simp add: conexion-def) auto  
**moreover**  
**let** ?C1 = A2  
**from** hip-aux **and** incidente-A2-a1 **and** incidente-B2-b1  
**have** incidente ?C1 a1  $\wedge$  incidente ?C1 b1 **by** simp  
**moreover**  
**let** ?C3 = A2  
**from** hip-aux **and** incidente-A2-a3 **and** incidente-B2-b3  
**have** incidente ?C3 a3  $\wedge$  incidente ?C3 b3 **by** simp  
**ultimately**  
**show** ?thesis **by** auto  
**qed**  
**next**  
**assume** hip-aux: A3=B3  
**show** ?thesis  
**proof** –  
**have**  $\exists C3$ . interseccion C3 a3 b3 **by** (rule existencia-interseccion)  
**then obtain** C3 **where** incidente C3 a3  $\wedge$  incidente C3 b3  
**by** (simp add: interseccion-def) auto  
**moreover**  
**have**  $\exists l$ . conexion l C3 A3 **by** (simp add: existencia-conexion)  
**then obtain** l **where** incidente C3 l  $\wedge$  incidente A3 l  
**by** (simp add: conexion-def) auto  
**moreover**  
**let** ?C1 = A3  
**from** hip-aux **and** incidente-A3-a1 **and** incidente-B3-b1  
**have** incidente ?C1 a1  $\wedge$  incidente ?C1 b1 **by** simp  
**moreover**  
**let** ?C2 = A3  
**from** hip-aux **and** incidente-A3-a2 **and** incidente-B3-b2  
**have** incidente ?C2 a2  $\wedge$  incidente ?C2 b2 **by** simp  
**ultimately**

show ?thesis by auto  
qed  
qed  
qed  
qed

**Lema 9.6.3 (desargues2a)** Sean  $X, Y, Z, A, B, C, P$  puntos;  $x, y, z, a, b, c, c_1, c_2, c_3$  rectas tales que,  $X = Y$  y  $X \neq Z$ ;  $A \neq B \vee A \neq C \vee B \neq C$ ;  $X$  es incidente con  $y, z, c_1$ ;  $Y$  es incidente con  $z, x, c_2$ ;  $Z$  es incidente con  $x, y, c_3$ ;  $A$  es incidente con  $b, c, c_1$ ;  $B$  es incidente con  $c, a, c_2$ ;  $C$  es incidente con  $a, b, c_3$ ;  $P$  es incidente con  $c_1, c_2, c_3$ . Entonces, existen tres puntos  $C_1, C_2, C_3$  y una recta  $l$  tales que  $C_1$  es incidente con  $x, a, l$ ;  $C_2$  es incidente con  $y, b, l$ ;  $C_3$  es incidente con  $z, c, l$ .

**Demostración:** Puesto que  $X = Y$  entonces, de la hipótesis  $Y$  es incidente con  $x$ , tenemos que  $X$  es incidente con  $x$ , además por hipótesis  $X \neq Z$ ,  $Z$  es incidente con  $x$ , y  $X, Z$  son incidentes con  $y$ , luego, por el axioma (V1b),  $x = y$ .

Por el principio del tercero excluido se tiene que,  $X = P \vee X \neq P$ . De lo anterior, demostramos por casos el lema.

1) Supongamos que  $X = P$ . Usando que  $P$  es incidente con  $c_3$  obtenemos que  $X$  es incidente con  $c_3$ , además, con las hipótesis,  $X \neq Z$ ;  $X$  y  $Z$  incidentes con  $x$ ,  $Z$  incidente con  $c_3$ , concluimos por el axioma (V1b) que  $x = c_3$ . De esto último, de  $x = y$  y de la hipótesis  $C$  es incidente con  $a, b, c_3$ , concluimos que  $C$  incidente con  $x, y, a, b$ .

Por otro lado, sea  $C_3$  el punto de intersección de  $z$  y  $c$ , y  $l$  la recta de conexión de  $C$  y  $C_3$ , entonces  $C_3$  es incidente con  $z, c, l$  y  $C$  es incidente con  $l$ .

En total, tenemos que  $C$  es incidente con  $x, y, a, b, l$  y  $C_3$  es incidente con  $z, c, l$ . De esta forma, haciendo  $C_1 = C_2 = C$ , queda, para este caso, demostrado el lema (ver Figura 9.11).

2) Supongamos que  $X \neq P$ . Puesto que  $X = Y$  entonces, de la hipótesis  $Y$  es incidente con  $c_2$ , tenemos que  $X$  es incidente con  $c_2$ , además sabemos que,  $X \neq P$ ;  $X, P$  son incidentes con  $c_1$ ;  $X$  es incidente con  $c_2$ , por lo tanto, por el axioma (V1b),  $c_1 = c_2$ .

Por el principio del tercero excluido se tiene que,  $A = B \vee A \neq B$ . De lo anterior, demostramos por casos el lema.

2.1) Supongamos que  $A = B$ . De lo anterior, y puesto que  $B$  es incidente con  $a$ , tenemos que  $A$  es incidente con  $a$ , y puesto que  $A \neq B \vee A \neq C \vee B \neq C$  tenemos que  $A \neq C$ . Además, usando las hipótesis  $C$  es incidente con  $a$  y  $A, C$  son incidentes con  $b$ , tenemos que, por el axioma (V1b),  $a = b$ .

Por otro lado, sea  $C_1$  el punto de intersección de  $x$  y  $a$ , Entonces  $C_1$  es incidente con  $x, a$  y como  $x = y$  y  $a = b$ , tenemos que  $C_1$  es incidente con  $x, a, y, b$ . Sea  $C_3$  el punto

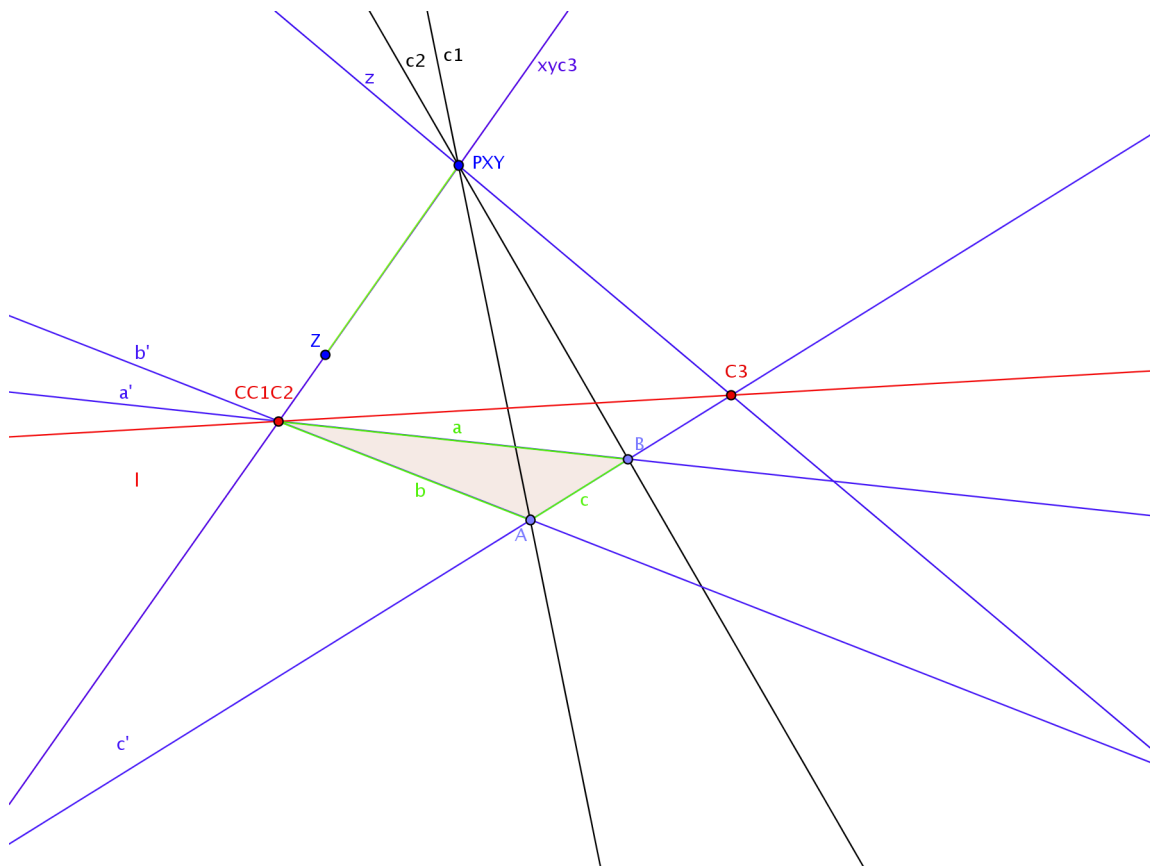


Figura 9.11: Lema 9.6.3



de intersección de  $z$  y  $c$ , entonces  $C_3$  es incidente con  $z, c$ . Por último, sea  $l$  la recta de conexión de  $C_1$  y  $C_3$ , entonces  $C_1, C_3$  son incidentes con  $l$ .

En total se tiene que  $C_1$  es incidente con  $x, a, y, b, l$  y  $C_3$  es incidente con  $z, c, l$ . De esta forma, haciendo  $C_2 = C_1$ , queda en este caso demostrado el lema (ver Figura 9.12).

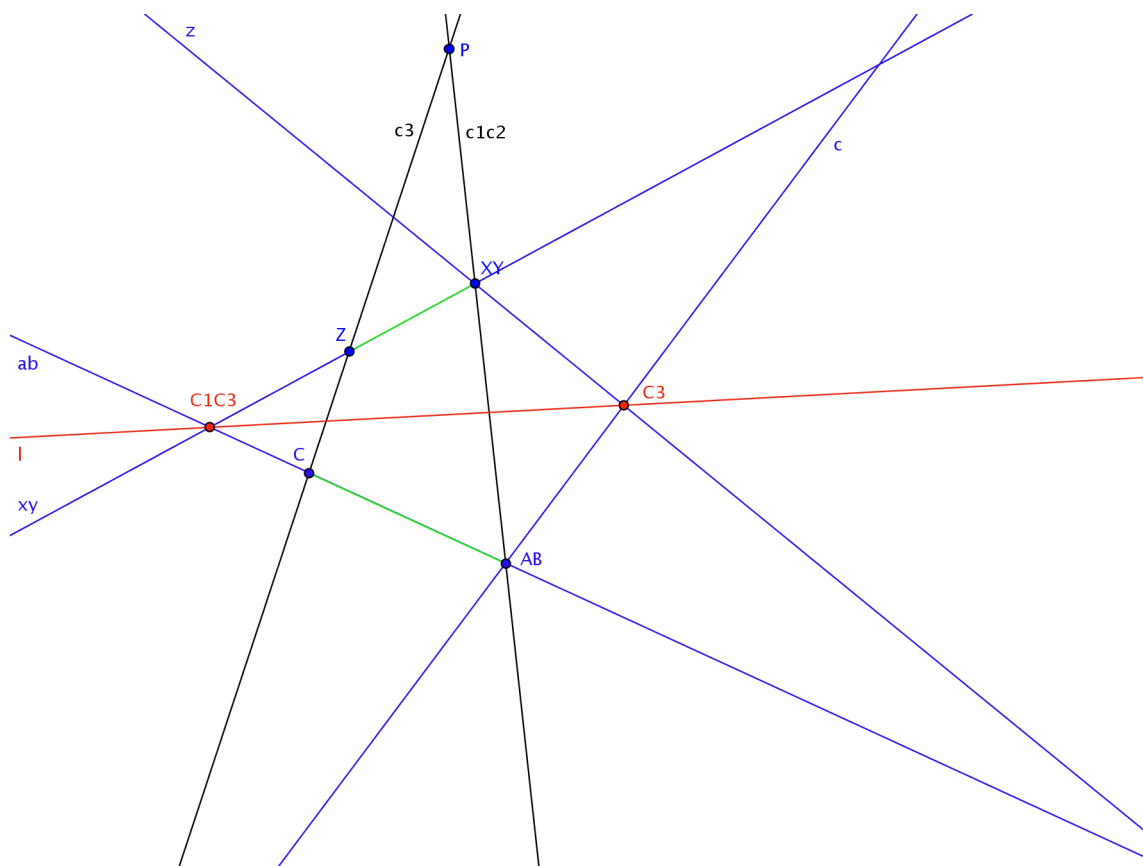


Figura 9.12: Lema 9.6.3

2.2) Supongamos que  $A \neq B$ . Puesto que  $c_1 = c_2$  entonces, de la hipótesis  $B$  es incidente con  $c_2$ , se tiene que  $B$  es incidente con  $c_1$ , además sabemos que  $A \neq B$ ,  $A$  es incidente con  $c$ , y  $A, B$  son incidentes con  $c_1$ , luego, por el axioma (V1b),  $c = c_1$ . De esto último y las hipótesis  $X$  es incidente con  $y, z, c_1$  tenemos que,  $X$  es incidente con  $z, c, x$ .

Por otro lado, sea  $C_1$  el punto de intersección de  $x$  y  $a$ , entonces  $C_1$  es incidente con  $x, a$ . Sea  $C_2$  el punto de intersección de  $y$  y  $b$ , entonces  $C_2$  es incidente con  $y, b$  y como  $x = y$ , tenemos que  $C_2$  es incidente con  $x, y, b$ .

En total, tenemos que  $X$  es incidente con  $z, c, x$ ;  $C_1$  es incidente con  $x, a$ ;  $C_2$  es incidente con  $x, y, b$ . De esta forma, haciendo  $C_3 = X$  y  $l = x$ , queda demostrado el lema (ver Figura 9.13).

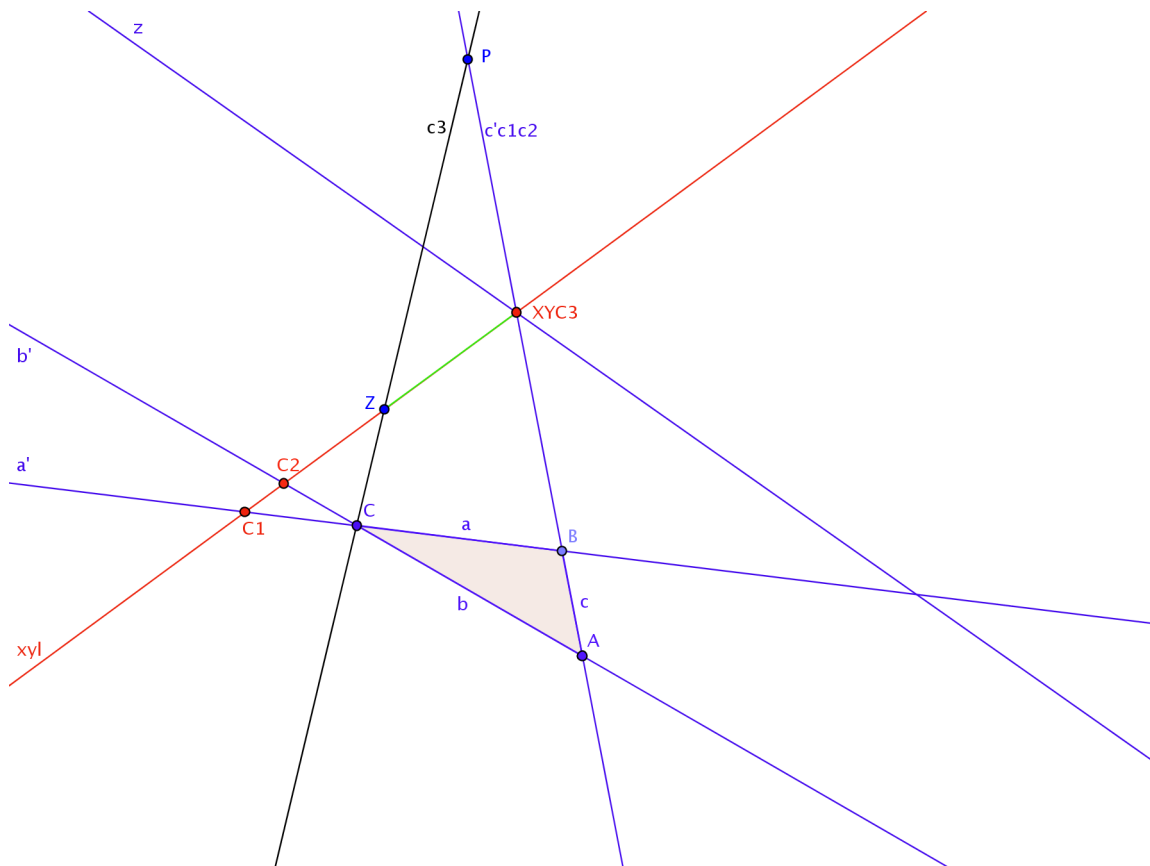


Figura 9.13: Lema 9.6.3

□

**lemma** *desargues2a*:

**assumes** *hip*:  $X = Y \wedge X \neq Z$   
**and** *no-coincidentes*:  $A \neq B \vee A \neq C \vee B \neq C$   
**and** *incidente-X-y*: *incidente*  $X y$   
**and** *incidente-X-z*: *incidente*  $X z$   
**and** *incidente-X-c1*: *incidente*  $X c1$   
**and** *incidente-Y-z*: *incidente*  $Y z$   
**and** *incidente-Y-x*: *incidente*  $Y x$   
**and** *incidente-Y-c2*: *incidente*  $Y c2$   
**and** *incidente-Z-x*: *incidente*  $Z x$   
**and** *incidente-Z-y*: *incidente*  $Z y$   
**and** *incidente-Z-c3*: *incidente*  $Z c3$   
**and** *incidente-A-b*: *incidente*  $A b$   
**and** *incidente-A-c*: *incidente*  $A c$   
**and** *incidente-A-c1*: *incidente*  $A c1$   
**and** *incidente-B-c*: *incidente*  $B c$   
**and** *incidente-B-a*: *incidente*  $B a$   
**and** *incidente-B-c2*: *incidente*  $B c2$   
**and** *incidente-C-a*: *incidente*  $C a$   
**and** *incidente-C-b*: *incidente*  $C b$   
**and** *incidente-C-c3*: *incidente*  $C c3$   
**and** *incidente-P-c1*: *incidente*  $P c1$   
**and** *incidente-P-c2*: *incidente*  $P c2$   
**and** *incidente-P-c3*: *incidente*  $P c3$   
**shows**  $\exists C1 C2 C3 l.$

*incidente*  $C1 x \wedge$  *incidente*  $C1 a \wedge$  *incidente*  $C1 l \wedge$   
*incidente*  $C2 y \wedge$  *incidente*  $C2 b \wedge$  *incidente*  $C2 l \wedge$   
*incidente*  $C3 z \wedge$  *incidente*  $C3 c \wedge$  *incidente*  $C3 l$

**proof** –

**from** *hip* **have** *iguales-X-Y*:  $X=Y$  **by** *simp*

**from** *hip* **have** *distintos-X-Z*:  $X \neq Z$  **by** *auto*

**moreover**

**from** *iguales-X-Y* **and** *incidente-Y-x* **have** *incidente-X-x*: *incidente*  $X x$  **by** *simp*

**moreover**

**from** *incidente-Z-x* **and** *incidente-X-y* **and** *incidente-Z-y* **have**

*incidente*  $Z x \wedge$  *incidente*  $X y \wedge$  *incidente*  $Z y$  **by** *simp*

**ultimately**

**have**

$X \neq Z \wedge$  (*incidente*  $X x \wedge$  *incidente*  $Z x$ )  $\wedge$  (*incidente*  $X y \wedge$  *incidente*  $Z y$ )

**by** *simp*

**hence** *iguales-x-y*:  $x=y$  **by** (*rule* *mp*[*OF axiomv1b*])

**have**  $X = P \vee X \neq P$  **by** *simp*  
**thus** *?thesis*  
**proof** *cases*  
**assume**  $X = P$   
**with** *incidente-P-c3* **have** *incidente-X-c3: incidente X c3* **by** *simp*  
**with** *distintos-X-Z* **and** *incidente-X-x* **and** *incidente-Z-x* **and** *incidente-Z-c3*  
**have**  $X \neq Z \wedge (\text{incidente } X \ x \wedge \text{incidente } Z \ x) \wedge (\text{incidente } X \ c3 \wedge \text{incidente } Z \ c3)$   
**by** *simp*  
**hence** *iguales-x-c3: x = c3* **by** (*rule mp[OF axiomv1b]*)  
**with** *incidente-C-c3* **have** *incidente-C-x: incidente C x* **by** *simp*  
**moreover**  
**with** *iguales-x-y* **and** *incidente-C-a* **and** *incidente-C-b*  
**have**  $\text{incidente } C \ y \wedge \text{incidente } C \ a \wedge \text{incidente } C \ b$  **by** *simp*  
**moreover**  
**have**  $\exists C3. \text{interseccion } C3 \ z \ c$  **by** (*rule existencia-interseccion*)  
**then obtain**  $C3$  **where** *incidente-C3-z-c: incidente C3 z  $\wedge$  incidente C3 c*  
**by** (*simp add: interseccion-def*) *auto*  
**moreover**  
**have**  $\exists l. \text{conexion } l \ C \ C3$  **by** (*simp add: existencia-conexion*)  
**then obtain**  $l$  **where** *incidente C l  $\wedge$  incidente C3 l*  
**by** (*simp add: conexion-def*) *auto*  
**ultimately**  
**show** *?thesis* **by** *auto*  
**next**  
**assume**  $X \neq P$   
**moreover**  
**from** *iguales-X-Y* **and** *incidente-Y-c2*  
**have** *incidente X c2* **by** *simp*  
**moreover**  
**from** *incidente-X-c1* **and** *incidente-P-c1* **and** *incidente-P-c2*  
**have**  
 $\text{incidente } X \ c1 \wedge \text{incidente } P \ c1 \wedge \text{incidente } P \ c2$  **by** *simp*  
**ultimately**  
**have**  $X \neq P \wedge (\text{incidente } X \ c1 \wedge \text{incidente } P \ c1) \wedge$   
 $(\text{incidente } X \ c2 \wedge \text{incidente } P \ c2)$  **by** *simp*  
**hence** *iguales-c1-c2: c1 = c2* **by** (*rule mp[OF axiomv1b]*)  
**have**  $A = B \vee A \neq B$  **by** *simp*  
**thus** *?thesis*  
**proof** *cases*  
**assume** *iguales-A-B: A = B*  
**with** *incidente-B-a* **have** *incidente-A-a: incidente A a* **by** *simp*  
**moreover**  
**from** *iguales-A-B* **and** *no-coincidentes* **have** *distintos-A-C: A  $\neq$  C* **by** *simp*

**moreover**

**from** *incidente-A-b* **and** *incidente-C-a* **and** *incidente-C-b* **have**

*incidente A b*  $\wedge$  *incidente C a*  $\wedge$  *incidente C b* **by** *simp*

**ultimately**

**have**

$A \neq C \wedge (\textit{incidente A a} \wedge \textit{incidente C a}) \wedge (\textit{incidente A b} \wedge \textit{incidente C b})$

**by** *simp*

**hence** *iguales-a-b: a=b* **by** (*rule mp[OF axiomv1b]*)

**moreover**

**have**  $\exists C1.$  *interseccion C1 x a* **by** (*rule existencia-interseccion*)

**then obtain** *C1* **where** *incidente C1 x*  $\wedge$  *incidente C1 a*

**by** (*simp add: interseccion-def*) *auto*

**moreover**

**with** *iguales-x-y* **and** *iguales-a-b*

**have** *incidente C1 y*  $\wedge$  *incidente C1 b* **by** *simp*

**moreover**

**have**  $\exists C3.$  *interseccion C3 z c* **by** (*rule existencia-interseccion*)

**then obtain** *C3* **where** *incidente C3 z*  $\wedge$  *incidente C3 c*

**by** (*simp add: interseccion-def*) *auto*

**moreover**

**have**  $\exists l.$  *conexion l C1 C3* **by** (*simp add: existencia-conexion*)

**then obtain** *l* **where** *incidente C1 l*  $\wedge$  *incidente C3 l*

**by** (*simp add: conexion-def*) *auto*

**ultimately**

**show** *?thesis* **by** *auto*

**next**

**assume** *hip-aux: A*  $\neq$  *B*

**from** *incidente-B-c2* **and** *iguales-c1-c2*

**have** *incidente B c1* **by** *simp*

**with** *hip-aux* **and** *incidente-A-c* **and** *incidente-B-c* **and** *incidente-B-c2*

**have**  $A \neq B \wedge (\textit{incidente A c} \wedge \textit{incidente B c}) \wedge$

$(\textit{incidente A c1} \wedge \textit{incidente B c1})$  **by** *simp*

**hence**  $c = c1$  **by** (*rule mp[OF axiomv1b]*)

**with** *incidente-X-c1* **have** *incidente X c* **by** *simp*

**with** *incidente-X-x* **and** *incidente-X-z*

**have** *incidente X z*  $\wedge$  *incidente X c*  $\wedge$  *incidente X x* **by** *simp*

**moreover**

**have**  $\exists C1.$  *interseccion C1 x a* **by** (*rule existencia-interseccion*)

**then obtain** *C1* **where** *incidente-C1-x-a: incidente C1 x*  $\wedge$  *incidente C1 a*

**by** (*simp add: interseccion-def*) *auto*

**moreover**

**have**  $\exists C2.$  *interseccion C2 y b* **by** (*rule existencia-interseccion*)

**then obtain**  $C_2$  **where**  $\text{incidente } C_2 \text{ y } \wedge \text{incidente } C_2 \text{ b}$   
**by** (*simp add: interseccion-def*) *auto*  
**with** *iguales-x-y*  
**have**  $\text{incidente } C_2 \text{ x } \wedge \text{incidente } C_2 \text{ y } \wedge \text{incidente } C_2 \text{ b}$  **by** *simp*  
**ultimately show** *?thesis* **by** *auto*  
**qed**  
**qed**  
**qed**

**Lema 9.6.4 (desargues2b)** Sean  $X, Y, Z, A, B, C, P$  puntos y  $x, y, z, a, b, c, c_1, c_2, c_3$  rectas tales que,  $X = Z$  y  $X \neq Y$ ;  $A \neq B \vee A \neq C \vee B \neq C$ ;  $X$  es incidente con  $y, z, c_1$ ;  $Y$  es incidente con  $z, x, c_2$ ;  $Z$  es incidente con  $x, y, c_3$ ;  $A$  es incidente con  $b, c, c_1$ ;  $B$  es incidente con  $c, a, c_2$ ;  $C$  es incidente con  $a, b, c_3$ ;  $P$  es incidente con  $c_1, c_2, c_3$ . Entonces, existen tres puntos  $C_1, C_2, C_3$  y una recta  $l$  tales que  $C_1$  es incidente con  $x, a, l$ ;  $C_2$  es incidente con  $y, b, l$ ;  $C_3$  es incidente con  $z, c, l$ .

**Demostración:** La demostración es análoga a la del lema 9.6.3. □

**lemma desargues2b:**

**assumes** *hip*:  $X = Z \wedge X \neq Y$   
**and** *no-coincidentes-B*:  $A \neq B \vee A \neq C \vee B \neq C$   
**and** *incidente-X-y*:  $\text{incidente } X \text{ y}$   
**and** *incidente-X-z*:  $\text{incidente } X \text{ z}$   
**and** *incidente-X-c1*:  $\text{incidente } X \text{ c1}$   
**and** *incidente-Y-z*:  $\text{incidente } Y \text{ z}$   
**and** *incidente-Y-x*:  $\text{incidente } Y \text{ x}$   
**and** *incidente-Y-c2*:  $\text{incidente } Y \text{ c2}$   
**and** *incidente-Z-x*:  $\text{incidente } Z \text{ x}$   
**and** *incidente-Z-y*:  $\text{incidente } Z \text{ y}$   
**and** *incidente-Z-c3*:  $\text{incidente } Z \text{ c3}$   
**and** *incidente-A-b*:  $\text{incidente } A \text{ b}$   
**and** *incidente-A-c*:  $\text{incidente } A \text{ c}$   
**and** *incidente-A-c1*:  $\text{incidente } A \text{ c1}$   
**and** *incidente-B-c*:  $\text{incidente } B \text{ c}$   
**and** *incidente-B-a*:  $\text{incidente } B \text{ a}$   
**and** *incidente-B-c2*:  $\text{incidente } B \text{ c2}$   
**and** *incidente-C-a*:  $\text{incidente } C \text{ a}$   
**and** *incidente-C-b*:  $\text{incidente } C \text{ b}$   
**and** *incidente-C-c3*:  $\text{incidente } C \text{ c3}$   
**and** *incidente-P-c1*:  $\text{incidente } P \text{ c1}$   
**and** *incidente-P-c2*:  $\text{incidente } P \text{ c2}$   
**and** *incidente-P-c3*:  $\text{incidente } P \text{ c3}$

**shows**  $\exists C1 C2 C3 l$ .

*incidente C1 x*  $\wedge$  *incidente C1 a*  $\wedge$  *incidente C1 l*  $\wedge$

*incidente C2 y*  $\wedge$  *incidente C2 b*  $\wedge$  *incidente C2 l*  $\wedge$

*incidente C3 z*  $\wedge$  *incidente C3 c*  $\wedge$  *incidente C3 l*

**proof** –

**from** *hip* **have** *iguales-X-Z*:  $X=Z$  **by** *simp*

**from** *hip* **have** *distintos-X-Y*:  $X \neq Y$  **by** *auto*

**moreover**

**from** *iguales-X-Z* **and** *incidente-Z-x* **have** *incidente-X-x*: *incidente X x* **by** *simp*

**moreover**

**from** *incidente-X-z* **and** *incidente-Y-x* **and** *incidente-Y-z* **have**

*incidente X z*  $\wedge$  *incidente Y x*  $\wedge$  *incidente Y z* **by** *simp*

**ultimately**

**have**

$X \neq Y \wedge (\textit{incidente X x} \wedge \textit{incidente Y x}) \wedge (\textit{incidente X z} \wedge \textit{incidente Y z})$

**by** *simp*

**hence** *iguales-x-z*:  $x=z$  **by** (*rule mp[OF axiomv1b]*)

**have**  $X = P \vee X \neq P$  **by** *simp*

**thus** *?thesis*

**proof** *cases*

**assume**  $X = P$

**with** *incidente-P-c2* **have** *incidente-X-c2*: *incidente X c2* **by** *simp*

**with** *distintos-X-Y* **and** *incidente-X-x* **and** *incidente-Y-x* **and** *incidente-Y-c2*

**have**  $X \neq Y \wedge (\textit{incidente X x} \wedge \textit{incidente Y x}) \wedge (\textit{incidente X c2} \wedge \textit{incidente Y c2})$

**by** *simp*

**hence** *iguales-x-c2*:  $x = c2$  **by** (*rule mp[OF axiomv1b]*)

**with** *incidente-B-c2* **have** *incidente B x* **by** *simp*

**moreover**

**with** *iguales-x-z* **and** *incidente-B-a* **and** *incidente-B-c*

**have** *incidente B z*  $\wedge$  *incidente B a*  $\wedge$  *incidente B c* **by** *simp*

**moreover**

**have**  $\exists C2$ . *interseccion C2 y b* **by** (*rule existencia-interseccion*)

**then obtain**  $C2$  **where** *incidente-C2-y-b*: *incidente C2 y*  $\wedge$  *incidente C2 b*

**by** (*simp add: interseccion-def*) *auto*

**moreover**

**have**  $\exists l$ . *conexion l B C2* **by** (*simp add: existencia-conexion*)

**then obtain**  $l$  **where** *incidente B l*  $\wedge$  *incidente C2 l*

**by** (*simp add: conexion-def*) *auto*

**moreover**

**ultimately**

**show** *?thesis* **by** *auto*

**next**

**assume**  $X \neq P$

**moreover**  
**from** *iguales-X-Z* **and** *incidente-Z-c3*  
**have** *incidente X c3* **by** *simp*  
**moreover**  
**from** *incidente-X-c1* **and** *incidente-P-c1* **and** *incidente-P-c3*  
**have**  
*incidente X c1*  $\wedge$  *incidente P c1*  $\wedge$  *incidente P c3* **by** *simp*  
**ultimately**  
**have**  $X \neq P \wedge (incidente X c1 \wedge incidente P c1) \wedge$   
 $(incidente X c3 \wedge incidente P c3)$  **by** *simp*  
**hence** *iguales-c1-c3: c1 = c3* **by** (*rule mp[OF axiomv1b]*)  
**have**  $A = C \vee A \neq C$  **by** *simp*  
**thus** *?thesis*  
**proof** *cases*  
**assume** *iguales-A-C: A = C*  
**with** *incidente-C-a* **have** *incidente-A-a: incidente A a* **by** *simp*  
**moreover**  
**from** *iguales-A-C* **and** *no-coincidentes-B* **have** *distintos-A-B: A ≠ B* **by** *simp*  
**moreover**  
**from** *incidente-A-c* **and** *incidente-B-a* **and** *incidente-B-c* **have**  
*incidente A c*  $\wedge$  *incidente B a*  $\wedge$  *incidente B c* **by** *simp*  
**ultimately**  
**have**  
 $A \neq B \wedge (incidente A a \wedge incidente B a) \wedge (incidente A c \wedge incidente B c)$   
**by** *simp*  
**hence** *iguales-a-c: a=c* **by** (*rule mp[OF axiomv1b]*)  
**moreover**  
**have**  $\exists C1. interseccion C1 x a$  **by** (*rule existencia-interseccion*)  
**then obtain** *C1* **where** *incidente C1 x*  $\wedge$  *incidente C1 a*  
**by** (*simp add: interseccion-def*) *auto*  
**moreover**  
**with** *iguales-x-z* **and** *iguales-a-c*  
**have** *incidente C1 z*  $\wedge$  *incidente C1 c* **by** *simp*  
**moreover**  
**have**  $\exists C2. interseccion C2 y b$  **by** (*rule existencia-interseccion*)  
**then obtain** *C2* **where** *incidente C2 y*  $\wedge$  *incidente C2 b*  
**by** (*simp add: interseccion-def*) *auto*  
**moreover**  
**have**  $\exists l. conexion l C1 C2$  **by** (*simp add: existencia-conexion*)  
**then obtain** *l* **where** *incidente C1 l*  $\wedge$  *incidente C2 l*  
**by** (*simp add: conexion-def*) *auto*  
**ultimately**  
**show** *?thesis* **by** *auto*



```

next
assume hip-aux: A≠C
from incidente-C-c3 and iguales-c1-c3
have incidente C c1 by simp
with hip-aux and incidente-A-b and incidente-C-b and incidente-A-c1
have A≠C ∧ (incidente A b ∧ incidente C b) ∧
  (incidente A c1 ∧ incidente C c1) by simp
hence b = c1 by (rule mp[OF axiom01b])
with incidente-X-c1 have incidente X b by simp
with incidente-X-x and incidente-X-y
have incidente X y ∧ incidente X b ∧ incidente X x by simp
moreover
have ∃ C1. interseccion C1 x a by (rule existencia-interseccion)
then obtain C1 where incidente-C1-x-a: incidente C1 x ∧ incidente C1 a
  by (simp add: interseccion-def) auto
moreover
have ∃ C3. interseccion C3 z c by (rule existencia-interseccion)
then obtain C3 where incidente C3 z ∧ incidente C3 c
  by (simp add: interseccion-def) auto
with iguales-x-z
have incidente C3 x ∧ incidente C3 z ∧ incidente C3 c by simp
ultimately show ?thesis by auto
qed
qed
qed

```

**Lema 9.6.5 (desargues2c)** Sean  $X, Y, Z, A, B, C, P$  puntos y  $x, y, z, a, b, c, c_1, c_2, c_3$  rectas tales que,  $Y = Z$  y  $Y \neq X$ ;  $A \neq B \vee A \neq C \vee B \neq C$ ;  $X$  es incidente con  $y, z, c_1$ ;  $Y$  es incidente con  $z, x, c_2$ ;  $Z$  es incidente con  $x, y, c_3$ ;  $A$  es incidente con  $b, c, c_1$ ;  $B$  es incidente con  $c, a, c_2$ ;  $C$  es incidente con  $a, b, c_3$ ;  $P$  es incidente con  $c_1, c_2, c_3$ . Entonces, existen tres puntos  $C_1, C_2, C_3$  y una recta  $l$  tales que  $C_1$  es incidente con  $x, a, l$ ;  $C_2$  es incidente con  $y, b, l$ ;  $C_3$  es incidente con  $z, c, l$ .

**Demostración:** La demostración es análoga a la del lema 9.6.3. □

**lemma desargues2c:**

```

assumes hip: Y = Z ∧ Y ≠ X
and no-coincidentes-B: A ≠ B ∨ A ≠ C ∨ B ≠ C
and incidente-X-y: incidente X y
and incidente-X-z: incidente X z
and incidente-X-c1: incidente X c1
and incidente-Y-z: incidente Y z

```

**and** *incidente-Y-x*: *incidente Y x*  
**and** *incidente-Y-c2*: *incidente Y c2*  
**and** *incidente-Z-x*: *incidente Z x*  
**and** *incidente-Z-y*: *incidente Z y*  
**and** *incidente-Z-c3*: *incidente Z c3*  
**and** *incidente-A-b*: *incidente A b*  
**and** *incidente-A-c*: *incidente A c*  
**and** *incidente-A-c1*: *incidente A c1*  
**and** *incidente-B-c*: *incidente B c*  
**and** *incidente-B-a*: *incidente B a*  
**and** *incidente-B-c2*: *incidente B c2*  
**and** *incidente-C-a*: *incidente C a*  
**and** *incidente-C-b*: *incidente C b*  
**and** *incidente-C-c3*: *incidente C c3*  
**and** *incidente-P-c1*: *incidente P c1*  
**and** *incidente-P-c2*: *incidente P c2*  
**and** *incidente-P-c3*: *incidente P c3*  
**shows**  $\exists C1 C2 C3 l$ .

*incidente C1 x*  $\wedge$  *incidente C1 a*  $\wedge$  *incidente C1 l*  $\wedge$   
*incidente C2 y*  $\wedge$  *incidente C2 b*  $\wedge$  *incidente C2 l*  $\wedge$   
*incidente C3 z*  $\wedge$  *incidente C3 c*  $\wedge$  *incidente C3 l*

**proof** –

**from** *hip* **have** *iguales-Y-Z*:  $Y=Z$  **by** *simp*

**from** *hip* **have** *distintos-Y-X*:  $Y \neq X$  **by** *auto*

**moreover**

**from** *iguales-Y-Z* **and** *incidente-Z-y* **have** *incidente-Y-y*: *incidente Y y* **by** *simp*

**moreover**

**from** *incidente-X-y* **and** *incidente-Y-z* **and** *incidente-X-z* **have**

*incidente X y*  $\wedge$  *incidente Y z*  $\wedge$  *incidente X z* **by** *simp*

**ultimately**

**have**

$Y \neq X \wedge (\text{incidente } Y y \wedge \text{incidente } X y) \wedge (\text{incidente } Y z \wedge \text{incidente } X z)$

**by** *simp*

**hence** *iguales-y-z*:  $y=z$  **by** (*rule mp*[*OF axiomv1b*])

**have**  $Y = P \vee Y \neq P$  **by** *simp*

**thus** *?thesis*

**proof** *cases*

**assume**  $Y = P$

**with** *incidente-P-c1* **have** *incidente-Y-c1*: *incidente Y c1* **by** *simp*

**with** *distintos-Y-X* **and** *incidente-Y-y* **and** *incidente-X-y* **and** *incidente-X-c1*

**have**  $Y \neq X \wedge (\text{incidente } Y y \wedge \text{incidente } X y) \wedge (\text{incidente } Y c1 \wedge \text{incidente } X c1)$

**by** *simp*

**hence** *iguales-y-c1*:  $y = c1$  **by** (*rule mp*[*OF axiomv1b*])

**with** *incidente-A-c1* **have** *incidente A y* **by** *simp*  
**moreover**  
**with** *iguales-y-z* **and** *incidente-A-b* **and** *incidente-A-c*  
**have**  $incidente\ A\ z \wedge incidente\ A\ b \wedge incidente\ A\ c$  **by** *simp*  
**moreover**  
**have**  $\exists\ C1.$  *interseccion C1 x a* **by** (*rule existencia-interseccion*)  
**then obtain** *C1* **where** *incidente-C1-x-a: incidente C1 x  $\wedge$  incidente C1 a*  
**by** (*simp add: interseccion-def*) *auto*  
**moreover**  
**have**  $\exists\ l.$  *conexion l A C1* **by** (*simp add: existencia-conexion*)  
**then obtain** *l* **where** *incidente A l  $\wedge$  incidente C1 l*  
**by** (*simp add: conexion-def*) *auto*  
**ultimately**  
**show** *?thesis* **by** *auto*  
**next**  
**assume**  $Y \neq P$   
**moreover**  
**from** *iguales-Y-Z* **and** *incidente-Z-c3*  
**have** *incidente Y c3* **by** *simp*  
**moreover**  
**from** *incidente-Y-c2* **and** *incidente-P-c2* **and** *incidente-P-c3*  
**have**  
*incidente Y c2  $\wedge$  incidente P c2  $\wedge$  incidente P c3* **by** *simp*  
**ultimately**  
**have**  $Y \neq P \wedge (incidente\ Y\ c2 \wedge incidente\ P\ c2) \wedge$   
 $(incidente\ Y\ c3 \wedge incidente\ P\ c3)$  **by** *simp*  
**hence** *iguales-c2-c3: c2 = c3* **by** (*rule mp[OF axiomv1b]*)  
**have**  $B = C \vee B \neq C$  **by** *simp*  
**thus** *?thesis*  
**proof** *cases*  
**assume** *iguales-B-C: B = C*  
**with** *incidente-C-b* **have** *incidente-B-b: incidente B b* **by** *simp*  
**moreover**  
**from** *iguales-B-C* **and** *no-coincidentes-B* **have** *distintos-B-A: B  $\neq$  A* **by** *simp*  
**moreover**  
**from** *incidente-A-b* **and** *incidente-B-c* **and** *incidente-A-c* **have**  
 $incidente\ A\ b \wedge incidente\ B\ c \wedge incidente\ A\ c$  **by** *simp*  
**ultimately**  
**have**  
 $B \neq A \wedge (incidente\ B\ b \wedge incidente\ A\ b) \wedge (incidente\ B\ c \wedge incidente\ A\ c)$   
**by** *simp*  
**hence** *iguales-b-c: b=c* **by** (*rule mp[OF axiomv1b]*)  
**moreover**

**have**  $\exists C1$ . *interseccion C1 x a* **by** (*rule existencia-interseccion*)  
**then obtain**  $C1$  **where** *incidente C1 x*  $\wedge$  *incidente C1 a*  
     **by** (*simp add: interseccion-def*) *auto*  
**moreover**  
**have**  $\exists C2$ . *interseccion C2 y b* **by** (*rule existencia-interseccion*)  
**then obtain**  $C2$  **where** *incidente C2 y*  $\wedge$  *incidente C2 b*  
     **by** (*simp add: interseccion-def*) *auto*  
**moreover**  
**with** *iguales-y-z* **and** *iguales-b-c*  
**have** *incidente C2 z*  $\wedge$  *incidente C2 c* **by** *simp*  
**moreover**  
**have**  $\exists l$ . *conexion l C1 C2* **by** (*simp add: existencia-conexion*)  
**then obtain**  $l$  **where** *incidente C1 l*  $\wedge$  *incidente C2 l*  
     **by** (*simp add: conexion-def*) *auto*  
**ultimately**  
**show** *?thesis* **by** *auto*  
**next**  
**assume** *hip-aux: B  $\neq$  C*  
**from** *incidente-C-c3* **and** *iguales-c2-c3*  
**have** *incidente C c2* **by** *simp*  
**with** *hip-aux* **and** *incidente-B-a* **and** *incidente-C-b* **and** *incidente-B-c2*  
**have**  $B \neq C \wedge$  (*incidente B a*  $\wedge$  *incidente C a*)  $\wedge$   
     (*incidente B c2*  $\wedge$  *incidente C c2*) **by** *simp*  
**hence**  $a = c2$  **by** (*rule mp[OF axiomv1b]*)  
**with** *incidente-Y-c2* **have** *incidente Y a* **by** *simp*  
**with** *incidente-Y-y* **and** *incidente-Y-z*  
**have** *incidente Y x*  $\wedge$  *incidente Y a*  $\wedge$  *incidente Y y* **by** *simp*  
**moreover**  
**have**  $\exists C2$ . *interseccion C2 y b* **by** (*rule existencia-interseccion*)  
**then obtain**  $C2$  **where** *incidente-C2-y-b: incidente C2 y*  $\wedge$  *incidente C2 b*  
     **by** (*simp add: interseccion-def*) *auto*  
**moreover**  
**have**  $\exists C3$ . *interseccion C3 z c* **by** (*rule existencia-interseccion*)  
**then obtain**  $C3$  **where** *incidente C3 z*  $\wedge$  *incidente C3 c*  
     **by** (*simp add: interseccion-def*) *auto*  
**with** *iguales-y-z*  
**have** *incidente C3 y*  $\wedge$  *incidente C3 z*  $\wedge$  *incidente C3 c* **by** *simp*  
**ultimately show** *?thesis* **by** *auto*  
**qed**  
**qed**  
**qed**

**Lema 9.6.6 (no-triang)** Sean  $X, Y, Z, A, B, C, P$  puntos y  $x, y, z, a, b, c, c_1, c_2, c_3$  rectas tales

que, el conjunto formado por los puntos  $X, Y, Z$  y las rectas  $x, y, z$  no es un triángulo;  $X \neq Y \vee X \neq Z \vee Y \neq Z$ ;  $A \neq B \vee A \neq C \vee B \neq C$ ;  $X$  es incidente con  $y, z, c_1$ ;  $Y$  es incidente con  $z, x, c_2$ ;  $Z$  es incidente con  $x, y, c_3$ ;  $A$  es incidente con  $b, c, c_1$ ;  $B$  es incidente con  $c, a, c_2$ ;  $C$  es incidente con  $a, b, c_3$ ;  $P$  es incidente con  $c_1, c_2, c_3$ . Entonces, existen tres puntos  $C_1, C_2, C_3$  y una recta  $l$  tales que  $C_1$  es incidente con  $x, a, l$ ;  $C_2$  es incidente con  $y, b, l$ ;  $C_3$  es incidente con  $z, c, l$ .

**Demostración:** Puesto que los puntos  $X, Y, Z$  y las rectas  $x, y, z$  no forman un triángulo, tenemos por definición que  $(X = Y \vee X = Z \vee Y = Z) \vee [(X \text{ no es incidente con } y) \vee (X \text{ no es incidente con } z) \vee (Y \text{ no es incidente con } x) \vee (Y \text{ no es incidente con } z) \vee (Z \text{ no es incidente con } x) \vee (Z \text{ no es incidente con } y)] \vee [(X \text{ es incidente con } x) \vee (Y \text{ es incidente con } y) \vee (Z \text{ es incidente con } z)]$ . A partir de esta hipótesis, demostramos por casos el lema.

1) Supongamos que  $X = Y \vee X = Z \vee Y = Z$ . Si  $X = Y$  entonces, como por hipótesis  $X \neq Y \vee X \neq Z \vee Y \neq Z$ , tenemos que  $X = Y \wedge X \neq Z$ , luego por el lema 9.6.3 se obtiene el resultado. Análogamente, si  $X = Z \vee Y = Z$  aplicando los lemas 9.6.4, 9.6.5 respectivamente, obtenemos la demostración del lema.

2) El caso  $(X \text{ no es incidente con } y) \vee (X \text{ no es incidente con } z) \vee (Y \text{ no es incidente con } x) \vee (Y \text{ no es incidente con } z) \vee (Z \text{ no es incidente con } x) \vee (Z \text{ no es incidente con } y)$ , es imposible; de lo contrario, si  $X$  no es incidente con  $y$  entonces con la hipótesis  $X$  es incidente con  $y$  obtenemos una contradicción. Análogamente, si suponemos cualquiera de los otros casos obtenemos una contradicción.

3) Supongamos que  $(X \text{ es incidente con } x) \vee (Y \text{ es incidente con } y) \vee (Z \text{ es incidente con } z)$ . La demostración es por casos.

3.1) Si  $X$  es incidente con  $x$ , usando la tautología  $X = Y \vee X \neq Y$  tenemos la siguiente demostración por casos.

3.1.1) Supongamos que  $X = Y$  entonces, de igual forma como lo demostrado en (1), se tiene la demostración del lema.

3.1.2) Si  $X \neq Y$ , usando la tautología  $X = Z \vee X \neq Z$  tenemos la siguiente demostración por casos.

3.1.2.1) Supongamos que  $X = Z$  entonces, de igual forma como lo demostrado en (1), se tiene en este caso la demostración del lema.

3.1.2.2) Supongamos que  $X \neq Z$ . De las hipótesis,  $X \neq Y$ ;  $X$  incidente con  $x, z$ ;  $Y$  incidente con  $y, z$ , tenemos que, por el axioma (V1b),  $x = z$ . De la misma forma, de las hipótesis,  $X \neq Z$ ;  $X$  incidente con  $x, y$ ;  $Z$  incidente con  $x, y$ , tenemos que, por el axioma (V1b),  $x = y$ . Ahora, sea  $C_1$  el punto de intersección de  $x$  y  $a$ , entonces  $C_1$  es incidente con  $x, a$ ; sea  $C_2$  el punto de intersección de  $x$  y  $b$ , entonces  $C_2$  es incidente con  $x, b$ ; sea  $C_3$  el punto de intersección de  $x$  y  $c$ , entonces  $C_3$  es incidente con  $x, c$ ;

En total, tenemos que existen  $C_1, C_2, C_3$  y  $l = x = y = z$  tales que satisfacen la conclusión del lema. Así, en este caso queda demostrado el lema.

Para los casos (3.b)  $Y$  es incidente con  $y$  y (3.c)  $Z$  es incidente con  $z$ , la demostración es análoga a la que se hizo en el caso (3.1). □

**lemma** *no-triang*:

**assumes** *no-triang*:  $\neg \text{triangulo } X Y Z x y z$

**and** *no-coincidentes-A*:  $X \neq Y \vee X \neq Z \vee Y \neq Z$

**and** *no-coincidentes-B*:  $A \neq B \vee A \neq C \vee B \neq C$

**and** *incidente-X-y*: *incidente*  $X y$

**and** *incidente-X-z*: *incidente*  $X z$

**and** *incidente-X-c1*: *incidente*  $X c1$

**and** *incidente-Y-z*: *incidente*  $Y z$

**and** *incidente-Y-x*: *incidente*  $Y x$

**and** *incidente-Y-c2*: *incidente*  $Y c2$

**and** *incidente-Z-x*: *incidente*  $Z x$

**and** *incidente-Z-y*: *incidente*  $Z y$

**and** *incidente-Z-c3*: *incidente*  $Z c3$

**and** *incidente-A-b*: *incidente*  $A b$

**and** *incidente-A-c*: *incidente*  $A c$

**and** *incidente-A-c1*: *incidente*  $A c1$

**and** *incidente-B-c*: *incidente*  $B c$

**and** *incidente-B-a*: *incidente*  $B a$

**and** *incidente-B-c2*: *incidente*  $B c2$

**and** *incidente-C-a*: *incidente*  $C a$

**and** *incidente-C-b*: *incidente*  $C b$

**and** *incidente-C-c3*: *incidente*  $C c3$

**and** *incidente-P-c1*: *incidente*  $P c1$

**and** *incidente-P-c2*: *incidente*  $P c2$

**and** *incidente-P-c3*: *incidente*  $P c3$

**shows**  $\exists C1 C2 C3 l$ .

*incidente*  $C1 x \wedge \text{incidente } C1 a \wedge \text{incidente } C1 l \wedge$

*incidente*  $C2 y \wedge \text{incidente } C2 b \wedge \text{incidente } C2 l \wedge$

*incidente*  $C3 z \wedge \text{incidente } C3 c \wedge \text{incidente } C3 l$

**proof** –

**from** *no-triang*

**have** *equivalente*:  $(X = Y \vee X = Z \vee Y = Z) \vee$

$\neg(\text{incidente } X y) \vee \neg(\text{incidente } X z) \vee$

$\neg(\text{incidente } Y x) \vee \neg(\text{incidente } Y z) \vee$

$\neg(\text{incidente } Z x) \vee \neg(\text{incidente } Z y) \vee$

$(\text{incidente } X x \vee \text{incidente } Y y \vee \text{incidente } Z z)$

**by** (*simp add: no-triangulo*)

**from** *equivalente* **show** ?thesis  
**proof** (rule disjE)  
**assume**  $X = Y \vee X = Z \vee Y = Z$   
**show** ?thesis  
**proof** (rule disjE)  
**assume** *hip-aux*:  $X = Y$   
**show** ?thesis  
**proof** –  
**from** *no-coincidentes-A* **and** *hip-aux*  
**have** *hip*:  $X=Y \wedge X \neq Z$  **by** *simp*  
**from** *desargues2a*[OF *hip no-coincidentes-B incidente-X-y incidente-X-z*  
*incidente-X-c1 incidente-Y-z incidente-Y-x incidente-Y-c2*  
*incidente-Z-x incidente-Z-y incidente-Z-c3 incidente-A-b*  
*incidente-A-c incidente-A-c1 incidente-B-c incidente-B-a*  
*incidente-B-c2 incidente-C-a incidente-C-b incidente-C-c3*  
*incidente-P-c1 incidente-P-c2 incidente-P-c3*]  
**show** ?thesis **by** *auto*  
**qed**  
**next**  
**assume**  $X = Z \vee Y = Z$   
**show** ?thesis  
**proof** (rule disjE)  
**assume** *hip-aux*:  $X = Z$   
**show** ?thesis  
**proof** –  
**from** *no-coincidentes-A* **and** *hip-aux*  
**have** *hip*:  $X=Z \wedge X \neq Y$  **by** *simp*  
**from** *desargues2b*[OF *hip no-coincidentes-B incidente-X-y incidente-X-z*  
*incidente-X-c1 incidente-Y-z incidente-Y-x incidente-Y-c2*  
*incidente-Z-x incidente-Z-y incidente-Z-c3 incidente-A-b*  
*incidente-A-c incidente-A-c1 incidente-B-c incidente-B-a*  
*incidente-B-c2 incidente-C-a incidente-C-b incidente-C-c3*  
*incidente-P-c1 incidente-P-c2 incidente-P-c3*]  
**show** ?thesis **by** *auto*  
**qed**  
**next**  
**assume** *hip-aux*:  $Y=Z$   
**show** ?thesis  
**proof** –  
**from** *no-coincidentes-A* **and** *hip-aux*  
**have** *hip*:  $Y=Z \wedge Y \neq X$  **by** *simp*  
**from** *desargues2c*[OF *hip no-coincidentes-B incidente-X-y incidente-X-z*  
*incidente-X-c1 incidente-Y-z incidente-Y-x incidente-Y-c2*

```

    incidente-Z-x incidente-Z-y incidente-Z-c3 incidente-A-b
    incidente-A-c incidente-A-c1 incidente-B-c incidente-B-a
    incidente-B-c2 incidente-C-a incidente-C-b incidente-C-c3
    incidente-P-c1 incidente-P-c2 incidente-P-c3]
  show ?thesis by auto
qed
qed
qed
next
assume  $\neg$  incidente X y  $\vee$   $\neg$  incidente X z  $\vee$   $\neg$  incidente Y x  $\vee$ 
   $\neg$  incidente Y z  $\vee$   $\neg$  incidente Z x  $\vee$   $\neg$  incidente Z y  $\vee$ 
  incidente X x  $\vee$  incidente Y y  $\vee$  incidente Z z
show ?thesis
proof (rule disjE)
  assume hip-aux:  $\neg$  incidente X y
  with incidente-X-y have False by simp
  thus ?thesis by simp
next
  assume  $\neg$  incidente X z  $\vee$   $\neg$  incidente Y x  $\vee$   $\neg$  incidente Y z  $\vee$ 
     $\neg$  incidente Z x  $\vee$   $\neg$  incidente Z y  $\vee$ 
    incidente X x  $\vee$  incidente Y y  $\vee$  incidente Z z
  show ?thesis
  proof (rule disjE)
    assume hip-aux:  $\neg$  incidente X z
    with incidente-X-z have False by simp
    thus ?thesis by simp
  next
    assume  $\neg$  incidente Y x  $\vee$   $\neg$  incidente Y z  $\vee$   $\neg$  incidente Z x  $\vee$ 
       $\neg$  incidente Z y  $\vee$ 
      incidente X x  $\vee$  incidente Y y  $\vee$  incidente Z z
    show ?thesis
    proof (rule disjE)
      assume hip-aux:  $\neg$  incidente Y x
      with incidente-Y-x have False by simp
      thus ?thesis by simp
    next
      assume  $\neg$  incidente Y z  $\vee$   $\neg$  incidente Z x  $\vee$   $\neg$  incidente Z y  $\vee$ 
        incidente X x  $\vee$  incidente Y y  $\vee$  incidente Z z
      show ?thesis
      proof (rule disjE)
        assume hip-aux:  $\neg$  incidente Y z
        with incidente-Y-z have False by simp
        thus ?thesis by simp
      
```



```

next
assume  $\neg$  incidente Z x  $\vee$   $\neg$  incidente Z y  $\vee$ 
  incidente X x  $\vee$  incidente Y y  $\vee$  incidente Z z
show ?thesis
proof (rule disjE)
  assume hip-aux:  $\neg$  incidente Z x
  with incidente-Z-x have False by simp
  thus ?thesis by simp
next
assume  $\neg$ incidente Z y  $\vee$ 
  incidente X x  $\vee$  incidente Y y  $\vee$  incidente Z z
show ?thesis
proof (rule disjE)
  assume hip-aux:  $\neg$  incidente Z y
  with incidente-Z-y have False by simp
  thus ?thesis by simp
next
assume incidente X x  $\vee$  incidente Y y  $\vee$  incidente Z z
show ?thesis
proof (rule disjE)
  assume incidente-X-x: incidente X x
  have casos: X=Y  $\vee$  X $\neq$ Y by simp
  thus ?thesis
proof cases
  assume X = Y
  with no-coincidentes-A
  have hip: X=Y  $\wedge$  X $\neq$  Z by simp
  from desargues2a[OF hip no-coincidentes-B incidente-X-y incidente-X-z
    incidente-X-c1 incidente-Y-z incidente-Y-x incidente-Y-c2
    incidente-Z-x incidente-Z-y incidente-Z-c3 incidente-A-b
    incidente-A-c incidente-A-c1 incidente-B-c incidente-B-a
    incidente-B-c2 incidente-C-a incidente-C-b incidente-C-c3
    incidente-P-c1 incidente-P-c2 incidente-P-c3]
  show ?thesis by auto
next
assume hip-aux1: X $\neq$ Y
  have casos1: X=Z  $\vee$  X $\neq$ Z by simp
  thus ?thesis
proof cases
  assume X=Z
  with no-coincidentes-A
  have hip: X=Z  $\wedge$  X $\neq$  Y by simp
  from desargues2b[OF hip no-coincidentes-B incidente-X-y incidente-X-z

```

*incidente-X-c1 incidente-Y-z incidente-Y-x incidente-Y-c2  
 incidente-Z-x incidente-Z-y incidente-Z-c3 incidente-A-b  
 incidente-A-c incidente-A-c1 incidente-B-c incidente-B-a  
 incidente-B-c2 incidente-C-a incidente-C-b incidente-C-c3  
 incidente-P-c1 incidente-P-c2 incidente-P-c3]*

**show** ?thesis **by** auto

**next**

**assume** *hip-aux2:  $X \neq Z$*

**from** *hip-aux1* **and** *incidente-X-x* **and** *incidente-X-z* **and**  
*incidente-Y-x* **and** *incidente-Y-z*

**have**

$X \neq Y \wedge (\text{incidente } X \ x \wedge \text{incidente } Y \ x) \wedge$   
 $(\text{incidente } X \ z \wedge \text{incidente } Y \ z)$  **by** simp

**hence**  $x = z$  **by** (rule mp[OF axiomv1b])

**moreover**

**from** *hip-aux2* **and** *incidente-X-x* **and** *incidente-X-y* **and**  
*incidente-Z-x* **and** *incidente-Z-y*

**have**

$X \neq Z \wedge (\text{incidente } X \ x \wedge \text{incidente } Z \ x) \wedge$   
 $(\text{incidente } X \ y \wedge \text{incidente } Z \ y)$  **by** simp

**hence**  $x = y$  **by** (rule mp[OF axiomv1b])

**moreover**

**have**  $\exists C1.$  *interseccion C1 x a* **by** (rule existencia-interseccion)

**then obtain** C1 **where**  $\text{incidente } C1 \ x \wedge \text{incidente } C1 \ a$   
**by** (simp add: interseccion-def) auto

**moreover**

**have**  $\exists C2.$  *interseccion C2 x b* **by** (rule existencia-interseccion)

**then obtain** C2 **where**  $\text{incidente } C2 \ x \wedge \text{incidente } C2 \ b$   
**by** (simp add: interseccion-def) auto

**moreover**

**have**  $\exists C3.$  *interseccion C3 x c* **by** (rule existencia-interseccion)

**then obtain** C3 **where**  $\text{incidente } C3 \ x \wedge \text{incidente } C3 \ c$   
**by** (simp add: interseccion-def) auto

**ultimately**

**show** ?thesis **by** auto

qed

qed

**next**

**assume** *incidente Y y*  $\vee$  *incidente Z z*

**show** ?thesis

**proof** (rule disjE)

**assume** *incidente-Y-y: incidente Y y*

**have** *casos:  $Y = X \vee Y \neq X$*  **by** simp

**thus** ?thesis  
**proof** cases  
**assume**  $Y = X$   
**with** no-coincidentes-A  
**have** hip:  $X=Y \wedge X \neq Z$  **by** simp  
**from**  
desargues2a[OF hip no-coincidentes-B incidente-X-y incidente-X-z  
incidente-X-c1 incidente-Y-z incidente-Y-x  
incidente-Y-c2 incidente-Z-x incidente-Z-y  
incidente-Z-c3 incidente-A-b incidente-A-c  
incidente-A-c1 incidente-B-c incidente-B-a  
incidente-B-c2 incidente-C-a incidente-C-b  
incidente-C-c3 incidente-P-c1 incidente-P-c2 incidente-P-c3]  
**show** ?thesis **by** auto  
**next**  
**assume** hip-aux1:  $Y \neq X$   
**have** casos1:  $Y=Z \vee Y \neq Z$  **by** simp  
**thus** ?thesis  
**proof** cases  
**assume**  $Y=Z$   
**with** no-coincidentes-A  
**have** hip:  $Y=Z \wedge Y \neq X$  **by** simp  
**from**  
desargues2c[OF hip no-coincidentes-B incidente-X-y incidente-X-z  
incidente-X-c1 incidente-Y-z incidente-Y-x incidente-Y-c2  
incidente-Z-x incidente-Z-y incidente-Z-c3 incidente-A-b  
incidente-A-c incidente-A-c1 incidente-B-c incidente-B-a  
incidente-B-c2 incidente-C-a incidente-C-b incidente-C-c3  
incidente-P-c1 incidente-P-c2 incidente-P-c3]  
**show** ?thesis **by** auto  
**next**  
**assume** hip-aux2:  $Y \neq Z$   
**from** hip-aux1 **and** incidente-Y-y **and** incidente-Y-z **and**  
incidente-X-y **and** incidente-X-z  
**have**  
 $Y \neq X \wedge (\text{incidente } Y \ y \wedge \text{incidente } X \ y) \wedge$   
 $(\text{incidente } Y \ z \wedge \text{incidente } X \ z)$  **by** simp  
**hence**  $y=z$  **by** (rule mp[OF axiom01b])  
**moreover**  
**from** hip-aux2 **and** incidente-Y-y **and** incidente-Y-x **and**  
incidente-Z-y **and** incidente-Z-x  
**have**  
 $Y \neq Z \wedge (\text{incidente } Y \ y \wedge \text{incidente } Z \ y) \wedge$

(*incidente Y x*  $\wedge$  *incidente Z x*) **by simp**  
**hence**  $y=x$  **by** (*rule mp*[OF *axiomv1b*])  
**moreover**  
**have**  $\exists C1$ . *interseccion C1 x a* **by** (*rule existencia-interseccion*)  
**then obtain**  $C1$  **where** *incidente C1 x*  $\wedge$  *incidente C1 a*  
     **by** (*simp add: interseccion-def*) *auto*  
**moreover**  
**have**  $\exists C2$ . *interseccion C2 x b* **by** (*rule existencia-interseccion*)  
**then obtain**  $C2$  **where** *incidente C2 x*  $\wedge$  *incidente C2 b*  
     **by** (*simp add: interseccion-def*) *auto*  
**moreover**  
**have**  $\exists C3$ . *interseccion C3 x c* **by** (*rule existencia-interseccion*)  
**then obtain**  $C3$  **where** *incidente C3 x*  $\wedge$  *incidente C3 c*  
     **by** (*simp add: interseccion-def*) *auto*  
**ultimately**  
**show** *?thesis* **by auto**  
**qed**  
**qed**  
**next**  
**assume** *incidente-Z-z: incidente Z z*  
**have** *casos: Z=X*  $\vee$  *Z*  $\neq$  *X* **by simp**  
**thus** *?thesis*  
**proof cases**  
   **assume**  $Z = X$   
   **with** *no-coincidentes-A*  
   **have** *hip: X=Z*  $\wedge$   $X \neq Y$  **by simp**  
   **from**  
     *desargues2b*[OF *hip no-coincidentes-B incidente-X-y incidente-X-z*  
       *incidente-X-c1 incidente-Y-z incidente-Y-x*  
       *incidente-Y-c2 incidente-Z-x incidente-Z-y*  
       *incidente-Z-c3 incidente-A-b incidente-A-c*  
       *incidente-A-c1 incidente-B-c incidente-B-a*  
       *incidente-B-c2 incidente-C-a incidente-C-b*  
       *incidente-C-c3 incidente-P-c1 incidente-P-c2 incidente-P-c3*]  
   **show** *?thesis* **by auto**  
**next**  
**assume** *hip-aux1: Z*  $\neq$  *X*  
**have** *casos1: Z=Y*  $\vee$  *Z*  $\neq$  *Y* **by simp**  
**thus** *?thesis*  
**proof cases**  
   **assume**  $Z=Y$   
   **with** *no-coincidentes-A*  
   **have** *hip: Y=Z*  $\wedge$   $Y \neq X$  **by simp**

```

from
  desargues2c[OF hip no-coincidentes-B incidente-X-y incidente-X-z
    incidente-X-c1 incidente-Y-z incidente-Y-x incidente-Y-c2
    incidente-Z-x incidente-Z-y incidente-Z-c3 incidente-A-b
    incidente-A-c incidente-A-c1 incidente-B-c incidente-B-a
    incidente-B-c2 incidente-C-a incidente-C-b incidente-C-c3
    incidente-P-c1 incidente-P-c2 incidente-P-c3]
show ?thesis by auto
next
assume hip-aux2:  $Z \neq Y$ 
from hip-aux1 and incidente-Z-z and incidente-X-z and
  incidente-Z-y and incidente-X-y
have
 $Z \neq X \wedge (\text{incidente } Z \ z \wedge \text{incidente } X \ z) \wedge$ 
  ( $\text{incidente } Z \ y \wedge \text{incidente } X \ y$ ) by simp
hence  $z=y$  by (rule mp[OF axiomv1b])
moreover
from hip-aux2 and incidente-Z-z and incidente-Z-x and
  incidente-Y-z and incidente-Y-x
have
 $Z \neq Y \wedge (\text{incidente } Z \ z \wedge \text{incidente } Y \ z) \wedge$ 
  ( $\text{incidente } Z \ x \wedge \text{incidente } Y \ x$ ) by simp
hence  $z=x$  by (rule mp[OF axiomv1b])
moreover
have  $\exists C1. \text{interseccion } C1 \ x \ a$  by (rule existencia-interseccion)
then obtain C1 where  $\text{incidente } C1 \ x \wedge \text{incidente } C1 \ a$ 
  by (simp add: interseccion-def) auto
moreover
have  $\exists C2. \text{interseccion } C2 \ x \ b$  by (rule existencia-interseccion)
then obtain C2 where  $\text{incidente } C2 \ x \wedge \text{incidente } C2 \ b$ 
  by (simp add: interseccion-def) auto
moreover
have  $\exists C3. \text{interseccion } C3 \ x \ c$  by (rule existencia-interseccion)
then obtain C3 where  $\text{incidente } C3 \ x \wedge \text{incidente } C3 \ c$ 
  by (simp add: interseccion-def) auto
ultimately
show ?thesis by auto
qed
qed
qed
qed
qed
qed

```

qed  
 qed  
 qed  
 qed  
 qed  
 qed

**Teorema 9.6.7 (desargues)** Supongamos que  $A_1 \neq A_2 \vee A_1 \neq A_3 \vee A_2 \neq A_3$ ;  $B_1 \neq B_2 \vee B_1 \neq B_3 \vee B_2 \neq B_3$ ;  $A_1$  es incidente con  $a_2, a_3, c_1$ ;  $A_2$  es incidente con  $a_3, a_1, c_2$ ;  $A_3$  es incidente con  $a_1, a_2, c_3$ ;  $B_1$  es incidente con  $b_2, b_3, c_1$ ;  $B_2$  es incidente con  $b_3, b_1, c_2$ ;  $B_3$  es incidente con  $b_1, b_2, c_3$ ; Entonces, existen tres puntos  $C_1, C_2, C_3$  y una recta  $l$  tales que  $C_1$  es incidente con  $a_1, b_1, l$ ;  $C_2$  es incidente con  $a_2, b_2, l$ ;  $C_3$  es incidente con  $a_3, b_3, l$ .

**Demostración:** Por el principio del tercero excluido tenemos que:

$$\begin{aligned} & [(triangulo A_1A_2A_3a_1a_2a_3 \wedge triangulo B_1B_2B_3b_1b_2b_3) \wedge \\ & (A_1 \neq B_1 \wedge A_2 \neq B_2 \wedge A_3 \neq B_3) \wedge (a_1 \neq b_1 \wedge a_2 \neq b_2 \wedge a_3 \neq b_3)] \vee \\ & \neg [(triangulo A_1A_2A_3a_1a_2a_3 \wedge triangulo B_1B_2B_3b_1b_2b_3) \wedge \\ & (A_1 \neq B_1 \wedge A_2 \neq B_2 \wedge A_3 \neq B_3) \wedge (a_1 \neq b_1 \wedge a_2 \neq b_2 \wedge a_3 \neq b_3)] \end{aligned}$$

A partir de esta tautología demostramos el teorema por casos.

1) Supongamos

$$\begin{aligned} & (triangulo A_1A_2A_3a_1a_2a_3 \wedge triangulo B_1B_2B_3b_1b_2b_3) \wedge \\ & (A_1 \neq B_1 \wedge A_2 \neq B_2 \wedge A_3 \neq B_3) \wedge (a_1 \neq b_1 \wedge a_2 \neq b_2 \wedge a_3 \neq b_3). \end{aligned}$$

De lo anterior y las hipótesis  $A_1, B_1, P$  son incidentes con  $c_1$ , y  $A_3, B_3, P$  son incidentes con  $c_3$ , utilizando el lema *desargues1a*, queda en este caso demostrado el teorema.

2) Supongamos

$$\begin{aligned} & \neg [(triangulo A_1A_2A_3a_1a_2a_3 \wedge triangulo B_1B_2B_3b_1b_2b_3) \wedge \\ & (A_1 \neq B_1 \wedge A_2 \neq B_2 \wedge A_3 \neq B_3) \wedge (a_1 \neq b_1 \wedge a_2 \neq b_2 \wedge a_3 \neq b_3)]. \end{aligned}$$

Lo anterior es equivalente a

$$\begin{aligned} & \neg (triangulo A_1A_2A_3a_1a_2a_3 \wedge triangulo B_1B_2B_3b_1b_2b_3) \vee \\ & \neg (A_1 \neq B_1 \wedge A_2 \neq B_2 \wedge A_3 \neq B_3) \vee \neg (a_1 \neq b_1 \wedge a_2 \neq b_2 \wedge a_3 \neq b_3). \end{aligned}$$

De aquí demostramos por casos el teorema.

2.a) Supongamos

$$\neg (triangulo A_1A_2A_3a_1a_2a_3 \wedge triangulo B_1B_2B_3b_1b_2b_3),$$

es decir,

$$\neg (triangulo A_1A_2A_3a_1a_2a_3) \vee \neg (triangulo B_1B_2B_3b_1b_2b_3).$$

En el caso  $\neg (triangulo A_1A_2A_3a_1a_2a_3)$  entonces con las hipótesis,  $A_1 \neq A_2 \vee A_1 \neq A_3 \vee A_2 \neq A_3$ ;  $B_1 \neq B_2 \vee B_1 \neq B_3 \vee B_2 \neq B_3$ ;  $A_1$  es incidente con  $a_2, a_3, c_1$ ;  $A_2$  es incidente con  $a_3, a_1, c_2$ ;  $A_3$  es incidente con  $a_1, a_2, c_3$ ;  $B_1$  es incidente con  $b_2, b_3, c_1$ ;  $B_2$  es incidente con  $b_3, b_1, c_2$ ;  $B_3$  es incidente con  $b_1, b_2, c_3$ ;  $P$  es incidente con  $c_1, c_2, c_3$ , por el lema *no-trian*, queda demostrado el teorema. En el caso  $\neg (triangulo B_1, B_2, B_3, b_1, b_2, b_3)$ , la demostración es igual a la anterior.

2.b) Supongamos

$\neg(A_1 \neq B_1 \wedge A_2 \neq B_2 \wedge A_3 \neq B_3) \vee \neg(a_1 \neq b_1 \wedge a_2 \neq b_2 \wedge a_3 \neq b_3)$ .

En el caso  $\neg(A_1 \neq B_1 \wedge A_2 \neq B_2 \wedge A_3 \neq B_3)$ , entonces con las hipótesis,  $A_1$  es incidente con  $a_2, a_3$ ;  $A_2$  es incidente con  $a_3, a_1$ ;  $A_3$  es incidente con  $a_1, a_2$ ;  $B_1$  es incidente con  $b_2, b_3$ ;  $B_2$  es incidente con  $b_3, b_1$ ;  $B_3$  es incidente con  $b_1, b_2$ , por el lema *desargues1c*, queda demostrado el teorema. En el caso  $\neg(a_1 \neq b_1 \wedge a_2 \neq b_2 \wedge a_3 \neq b_3)$ , usando el lema *desargues1b*, se tiene la prueba del teorema. □

**theorem** *desargues*:

**assumes** *no-coincidentes-A*:  $A_1 \neq A_2 \vee A_1 \neq A_3 \vee A_2 \neq A_3$

**and** *no-coincidentes-B*:  $B_1 \neq B_2 \vee B_1 \neq B_3 \vee B_2 \neq B_3$

**and** *incidente-A1-a2*: *incidente*  $A_1 a_2$

**and** *incidente-A1-a3*: *incidente*  $A_1 a_3$

**and** *incidente-A1-c1*: *incidente*  $A_1 c_1$

**and** *incidente-A2-a3*: *incidente*  $A_2 a_3$

**and** *incidente-A2-a1*: *incidente*  $A_2 a_1$

**and** *incidente-A2-c2*: *incidente*  $A_2 c_2$

**and** *incidente-A3-a1*: *incidente*  $A_3 a_1$

**and** *incidente-A3-a2*: *incidente*  $A_3 a_2$

**and** *incidente-A3-c3*: *incidente*  $A_3 c_3$

**and** *incidente-B1-b2*: *incidente*  $B_1 b_2$

**and** *incidente-B1-b3*: *incidente*  $B_1 b_3$

**and** *incidente-B1-c1*: *incidente*  $B_1 c_1$

**and** *incidente-B2-b3*: *incidente*  $B_2 b_3$

**and** *incidente-B2-b1*: *incidente*  $B_2 b_1$

**and** *incidente-B2-c2*: *incidente*  $B_2 c_2$

**and** *incidente-B3-b1*: *incidente*  $B_3 b_1$

**and** *incidente-B3-b2*: *incidente*  $B_3 b_2$

**and** *incidente-B3-c3*: *incidente*  $B_3 c_3$

**and** *incidente-P-c1*: *incidente*  $P c_1$

**and** *incidente-P-c2*: *incidente*  $P c_2$

**and** *incidente-P-c3*: *incidente*  $P c_3$

**shows**  $\exists C_1 C_2 C_3 l$ .

*incidente*  $C_1 a_1 \wedge$  *incidente*  $C_1 b_1 \wedge$  *incidente*  $C_1 l \wedge$

*incidente*  $C_2 a_2 \wedge$  *incidente*  $C_2 b_2 \wedge$  *incidente*  $C_2 l \wedge$

*incidente*  $C_3 a_3 \wedge$  *incidente*  $C_3 b_3 \wedge$  *incidente*  $C_3 l$

**proof** –

**have**  $((\text{triangulo } A_1 A_2 A_3 a_1 a_2 a_3 \wedge \text{triangulo } B_1 B_2 B_3 b_1 b_2 b_3) \wedge$

$(A_1 \neq B_1 \wedge A_2 \neq B_2 \wedge A_3 \neq B_3) \wedge (a_1 \neq b_1 \wedge a_2 \neq b_2 \wedge a_3 \neq b_3)) \vee$

$\neg((\text{triangulo } A_1 A_2 A_3 a_1 a_2 a_3 \wedge \text{triangulo } B_1 B_2 B_3 b_1 b_2 b_3) \wedge$

$(A_1 \neq B_1 \wedge A_2 \neq B_2 \wedge A_3 \neq B_3) \wedge (a_1 \neq b_1 \wedge a_2 \neq b_2 \wedge a_3 \neq b_3))$  **by** *auto*

**thus** *?thesis*

**proof cases**

**assume**  $(\text{triangulo } A1 \ A2 \ A3 \ a1 \ a2 \ a3 \wedge \text{ triangulo } B1 \ B2 \ B3 \ b1 \ b2 \ b3) \wedge$   
 $(A1 \neq B1 \wedge A2 \neq B2 \wedge A3 \neq B3) \wedge (a1 \neq b1 \wedge a2 \neq b2 \wedge a3 \neq b3)$

**hence** *triangulos*:  $(\text{triangulo } A1 \ A2 \ A3 \ a1 \ a2 \ a3 \wedge \text{ triangulo } B1 \ B2 \ B3 \ b1 \ b2 \ b3)$  **and**

*vertices-distintos*:  $A1 \neq B1 \wedge A2 \neq B2 \wedge A3 \neq B3$  **and** *lados-distintos*:  $a1 \neq b1 \wedge a2 \neq b2 \wedge a3 \neq b3$

**by auto**

**from** *desargues1a*[*OF triangulos vertices-distintos lados-distintos*  
*incidente-A1-c1 incidente-A2-c2 incidente-A3-c3*  
*incidente-B1-c1 incidente-B2-c2 incidente-B3-c3*  
*incidente-P-c1 incidente-P-c2 incidente-P-c3*]

**show** *?thesis* **by simp**

**next**

**assume**

$\neg((\text{triangulo } A1 \ A2 \ A3 \ a1 \ a2 \ a3 \wedge \text{ triangulo } B1 \ B2 \ B3 \ b1 \ b2 \ b3) \wedge$   
 $(A1 \neq B1 \wedge A2 \neq B2 \wedge A3 \neq B3) \wedge (a1 \neq b1 \wedge a2 \neq b2 \wedge a3 \neq b3))$

**hence**

$\neg(\text{triangulo } A1 \ A2 \ A3 \ a1 \ a2 \ a3 \wedge \text{ triangulo } B1 \ B2 \ B3 \ b1 \ b2 \ b3) \vee$   
 $\neg(A1 \neq B1 \wedge A2 \neq B2 \wedge A3 \neq B3) \vee \neg(a1 \neq b1 \wedge a2 \neq b2 \wedge a3 \neq b3)$  **by simp**

**thus** *?thesis*

**proof**(*rule disjE*)

**assume** *no-triangulos*:  $\neg(\text{triangulo } A1 \ A2 \ A3 \ a1 \ a2 \ a3 \wedge \text{ triangulo } B1 \ B2 \ B3 \ b1 \ b2 \ b3)$

**hence**  $(\neg \text{triangulo } A1 \ A2 \ A3 \ a1 \ a2 \ a3) \vee (\neg \text{ triangulo } B1 \ B2 \ B3 \ b1 \ b2 \ b3)$  **by simp**

**thus** *?thesis*

**proof** (*rule disjE*)

**assume** *no-trian*:  $\neg \text{triangulo } A1 \ A2 \ A3 \ a1 \ a2 \ a3$

**from** *no-triang*[*OF no-trian no-coincidentes-A no-coincidentes-B incidente-A1-a2*  
*incidente-A1-a3 incidente-A1-c1 incidente-A2-a3 incidente-A2-a1*  
*incidente-A2-c2 incidente-A3-a1 incidente-A3-a2 incidente-A3-c3*  
*incidente-B1-b2 incidente-B1-b3 incidente-B1-c1 incidente-B2-b3*  
*incidente-B2-b1 incidente-B2-c2 incidente-B3-b1 incidente-B3-b2*  
*incidente-B3-c3 incidente-P-c1 incidente-P-c2 incidente-P-c3*]

**show** *?thesis* **by auto**

**next**

**assume** *no-trian*:  $\neg \text{triangulo } B1 \ B2 \ B3 \ b1 \ b2 \ b3$

**from** *no-triang*[*OF no-trian no-coincidentes-B no-coincidentes-A incidente-B1-b2*  
*incidente-B1-b3 incidente-B1-c1 incidente-B2-b3 incidente-B2-b1*  
*incidente-B2-c2 incidente-B3-b1 incidente-B3-b2 incidente-B3-c3*  
*incidente-A1-a2 incidente-A1-a3 incidente-A1-c1 incidente-A2-a3*  
*incidente-A2-a1 incidente-A2-c2 incidente-A3-a1 incidente-A3-a2*  
*incidente-A3-c3 incidente-P-c1 incidente-P-c2 incidente-P-c3*]

**show** *?thesis* **by auto**

**qed**

**next**



```

assume  $\neg(A1 \neq B1 \wedge A2 \neq B2 \wedge A3 \neq B3) \vee \neg(a1 \neq b1 \wedge a2 \neq b2 \wedge a3 \neq b3)$ 
thus ?thesis
proof(rule disjE)
  assume no-vertices-distintos:  $\neg(A1 \neq B1 \wedge A2 \neq B2 \wedge A3 \neq B3)$ 
  from desargues1c[OF no-vertices-distintos
    incidente-A1-a2 incidente-A1-a3
    incidente-A2-a3 incidente-A2-a1
    incidente-A3-a1 incidente-A3-a2
    incidente-B1-b2 incidente-B1-b3
    incidente-B2-b3 incidente-B2-b1
    incidente-B3-b1 incidente-B3-b2]
  show ?thesis by simp
  next
  assume no-lados-distintos:  $\neg(a1 \neq b1 \wedge a2 \neq b2 \wedge a3 \neq b3)$ 
  from desargues1b[OF no-lados-distintos] show ?thesis by simp
qed
qed
qed
qed

```



# Capítulo 10

## Conclusiones

En los capítulos 1 y 2 se formalizaron en Isar los teoremas de Cantor y del punto fijo de Knaster-Tarski; las pruebas presentadas muestran las facilidades del lenguaje Isar para formalizar textualmente demostraciones clásicas de las matemáticas y de esta forma obtener pruebas semi-automáticas bien estructuradas.

Las pruebas en Isabelle son hechas en forma aplicativa (usando el comando *apply*), ver [6], y por lo tanto son poco descriptivas. Así, es conveniente interactuar con el sistema para poder tener una idea del razonamiento empleado en una prueba. Siguiendo esta metodología, en el capítulo 3 demostramos en Isar el teorema de Schröder-Bernstein a partir de la correspondiente demostración en Isabelle. En general, se pueden combinar ambos estilos de prueba, por ejemplo, si para una prueba en Isar estamos intentando emplear un paso automático y esto no es posible, o también en el proceso gradual de convertir una prueba en Isabelle en la correspondiente en Isar.

En el capítulo 4 los ejemplos estudiados sobre propiedades básicas de la teoría de grupos nos permitió mostrar cómo los métodos de deducción natural, incluyendo inducción, pueden ser combinados en Isar con los métodos de razonamiento ecuacional y de cálculo. De igual forma, las pruebas sobre números primos realizadas en el capítulo 5 muestran que las facilidades de poder integrar estas formas de razonamiento, nos permiten contar con técnicas estructuradas de pruebas algebraicas.

En el capítulo 6 se presentó la formalización de una propiedad sobre los números racionales e irracionales utilizando los mismos conceptos y resultados elementales usados en la demostración usual. Sin embargo, la formalización de estos conceptos y definiciones, que no es requerida en la prueba, sí está basada en pruebas más elaboradas que utilizan resultados específicos de las teorías desarrolladas en el sistema Isabelle. Por ejemplo, la formalización del número  $\sqrt{2}$  depende de que la función  $f(x) = \sqrt{x}$  esté bien definida, y para esto se utiliza la formalización del teorema del valor medio. De igual forma, la definición de la función exponencial  $\exp(x) = e^x$  utiliza la formalización del concepto de convergencia de series de potencias. En resumen, el lenguaje Isar per-

mite al usuario demostrar resultados elementales sin conocimiento específico acerca de la formalización de las matemáticas.

En el capítulo 7 se analizó y formalizó la demostración de una propiedad de funciones de valores reales, basada en la propiedad de completitud de los números reales, en la que no aparecen los detalles de la prueba. Desde el punto de vista pedagógico, el ejercicio de formalizar una demostración matemática, sirve para analizar los argumentos, propiedades y conceptos abstractos involucrados en la prueba. Esto en particular, es de gran utilidad en demostraciones que no justifican explícitamente los resultados utilizados.

En el capítulo 8 estudiamos la forma cómo la axiomatización de la geometría del plano proyectivo puede ser formalizada en Isar. Mostramos la forma de hacer pruebas formales constructivas e ilustramos cómo en contraste con la demostración matemática, la prueba mecánica, de incidencia entre puntos y rectas, requiere considerar explícitamente los diferentes casos. En general, los casos análogos o particulares que tradicionalmente no son probados en los textos de matemáticas, deben ser verificados en la prueba formal, garantizando de esta forma la confiabilidad de la demostración usual. Sin embargo al aumentar el tamaño de la prueba, su presentación se hace menos legible. Por otro lado, se introdujo el concepto de dualidad y se justificó que teóricamente los teoremas duales de teoremas ya probados no requieren de una demostración, sin embargo se evidenció que, en el caso de la prueba automática de teoremas, sí necesitan ser demostrados para poder ser usados en pruebas posteriores. Por último se formalizó la prueba de la proposición generalizada de Desargues descomponiendo la demostración por casos, en donde se resalta el trabajo técnico necesario para poder considerar formalmente los distintos casos de configuración de puntos y rectas.

# Bibliografía

- [1] P. R. Halmos. *Naive Set Theory*. Springer, 1974.
- [2] I. N. Herstein. *Topics in Algebra*. Springer, 1989.
- [3] A. Heyting. *Axiomatic Projective Geometry*. Elsevier Science Publishing, 1963.
- [4] A. Krauss. *Defining Recursive Functions in Isabelle/HOL*. <http://isabelle.in.tum.de/doc/functions.pdf>.
- [5] T. Nipkow. *A Tutorial Introduction to Structured Isar Proofs*. <http://isabelle.in.tum.de/dist/Isabelle/doc/isar-overview.pdf>.
- [6] T. Nipkow, L. C. Paulson, and M. Wenzel. *Isabelle/HOL: A proof assistant for higher-order logic*. Lecture notes in Computer Science, vol 2283, Springer-Verlag, 2002. <http://isabelle.in.tum.de/dist/Isabelle/doc/tutorial.pdf>.
- [7] L. C. Paulson. Set theory for verification: Ii. induction and recursion. Technical report, Comp. Lab., Univ. Camb., 1995. <http://www.cl.cam.ac.uk/~lp15/papers/Sets/set-II.pdf>.
- [8] M. Wenzel. *Calculational reasoning revisited - an Isabelle/Isar experience*. <http://www4.in.tum.de/~wenzelm/papers/Calculations-Isar.pdf>.
- [9] M. Wenzel. *Isabelle/Isar — a generic framework for human-readable proof documents*. <http://www4.in.tum.de/~wenzelm/papers/isar-framework.pdf>.
- [10] M. Wenzel. *The Isabelle/Isar Reference Manual*. <http://isabelle.in.tum.de/dist/Isabelle/doc/isar-ref.pdf>.
- [11] M. Wenzel. *Miscellaneous Isabelle/Isar examples for Higher-Order Logic*. [http://isabelle.in.tum.de/dist/library/HOL/Isar\\_examples/index.html](http://isabelle.in.tum.de/dist/library/HOL/Isar_examples/index.html).
- [12] M. Wenzel. Isar — a generic interpretative approach to readable formal proof documents. In Y. Bertot, G. Dowek, A. Hirschowitz, C. Paulin, and L. They, editors, *Theorem Proving in Higher Order Logics: TPHOLs '99*, LNCS 1690, 1999.

- [13] M. Wenzel. *Isabelle/Isar - a versatile environment for human-readable formal proof documents*. PhD thesis, Technische Universität München, 2002. <http://tumb1.biblio.tu-muenchen.de/publ/diss/in/2002/wenzel.html>.
- [14] M. Wenzel and L. C. Paulson. Isabelle/Isar. In Wiedijk [16].
- [15] F. Wiedijk. *Formalizing 100 theorems*. <http://www.cs.ru.nl/~freek/100/>.
- [16] F. Wiedijk, editor. *The Seventeen Provers of the World*, volume 3600 of LNAI, 2006.