Ejercicio 2.18 Consideremos una teoría T de primer orden con igualdad con los axiomas propios

$\forall X \forall Y\ \mathsf{f}(X,Y) = \mathsf{f}(Y,X)$
$\forall X \forall Y\ \mathsf{f}(\mathsf{f}(X,Y),Z) = \mathsf{f}(X,\mathsf{f}(Y,Z))$
$\forall X\ \mathsf{f}(\mathsf{g}(X),\mathsf{g}(X)) = \mathsf{g}(X)$
$\forall X\ \mathsf{p}(X,\mathsf{g}(X))$
$\forall X \forall Y(\mathsf{p}(X,Y) \rightarrow \mathsf{p}(X,\mathsf{f}(Y,Z)))$
$\mathsf{q}(\mathsf{a})$

Demostrar por refutación, empleando resolución y paramodulación,

$\forall X \forall Y\ \mathsf{p}(X,\mathsf{f}(\mathsf{g}(Y),\mathsf{f}(\mathsf{g}(X),\mathsf{g}(X))))$ ◁

Ejercicio 2.19 (vd. ejercicio 2.2). Sea X un conjunto ordenado mediante una relación de orden parcial $\leq$. Se dice que un elemento y de X es *maximal* de X si cualquier elemento x de X cumple: si $y \leq x$, entonces $x = y$. Se dice que un elemento y de X es *máximo* de X si para todo x de X se cumple que $x \leq y$. Se pide:

1. Expresar formalmente las definiciones de ser elemento maximal y máximo.

2. Demostrar empleando paramodulación y resolución que existe a lo sumo un elemento máximo.

◁

2.7.3. DEMODULACIÓN Y RESCRITURA.

El principio de "sustituir por cosas iguales" es el que, de una forma u otra, hemos empleado hasta este momento para razonar en teorías con igualdad. En la práctica, sin embargo, el principio que usamos, siempre que sea posible, es levemente diferente: lo que hacemos es "sustituir por cosas iguales, pero más simples". La concreción y formalización de este principio lleva a lo que se llama "sistemas de rescritura" (en los ambientes más teóricos) o "razonamiento por demodulación" (en los contextos más aplicados). Estos sistemas tienen gran importancia tanto teórica (pues a través de ellos se enlaza con problemas clásicos del Álgebra, como el *problema de la palabra*) como práctica (pues, a menos que se emplee alguna forma de demodulación, la explosión combinatoria rápidamente hace inviable razonar automáticamente en teorías con igualdad).

Definición 2.18 Correspondencia (matching). *Dados dos términos φ y ψ, se dice que ψ se corresponde con φ cuando existe una sustitución σ tal que $\psi = \varphi.\sigma$.*

Por ejemplo, $\mathsf{f}(\mathsf{f}(\mathsf{a}))$ se corresponde con $\mathsf{f}(X)$, pero no al contrario.

Definición 2.19 *Sea un lenguaje de primer orden $CP(\Omega)$. Sea $term(\Omega)$ el conjunto de sus términos. Una regla de rescritura es un par (izq, der), donde $izq \in term(\Omega)$, $der \in term(\Omega)$. Denotaremos una regla (izq, der) como $izq \Rightarrow der$.*

Un sistema de rescritura es un conjunto finito de reglas de rescritura.

Definición 2.20 *Sea R un sistema de rescritura y sea $r \in R$ de la forma $izq \Rightarrow der$. Sea $\varphi(t)$ un término en el que hay una aparición del término t, y sea t tal que t se corresponde con izq mediante la sustitución σ. Sea $\varphi(der.\sigma)$ el resultado de sustituir en $\varphi(t)$ esa aparición de t por $der\sigma$. Entonces se dice que $\varphi(der\sigma)$ es una rescritura de $\varphi(t)$ según r y se escribe $\varphi(t) \overset{r}{\Rightarrow} \varphi(der\sigma)$.*

Análogamente, si para alguna $r \in R$ se tiene $\varphi \Rightarrow r\psi$, entonces diremos que ψ es una rescritura de φ según R, y escribiremos $\varphi \overset{R}{\Rightarrow} \psi$.

Definición 2.21 *Sea R un sistema de rescritura. La relación de derivación $\overset{R*}{\Rightarrow}$ es la clausura reflexiva y transitiva de la relación $\overset{R}{\Rightarrow}$. La relación de similaridad $\overset{R}{\Leftrightarrow}$ es la clausura reflexiva, simétrica y transitiva de $\overset{R}{\Rightarrow}$.*

Es decir, dadas dos fórmulas o términos φ, ψ, se dice que ψ se deriva de φ, $\varphi \overset{R*}{\Rightarrow} \psi$, cuando existen n fórmulas $\varphi = \varphi_1$, φ_2,. . . , $\varphi n = \psi$ $(n \leq 0)$ tales que

$$\varphi_1 \overset{R}{\Rightarrow} \varphi_2 \overset{R}{\Rightarrow} \ldots \overset{R}{\Rightarrow} \varphi_n$$

Y se dice que φ y ψ son similares cuando existen n fórmulas $\varphi = \varphi_1$, φ_2,. . . , $\varphi n = \psi$ $(n \leq 0)$ tales que

$$\varphi_1 \left\{ \begin{array}{c} \overset{R}{\Rightarrow} \\ \overset{R}{\Leftarrow} \end{array} \right\} \varphi_2 \left\{ \begin{array}{c} \overset{R}{\Rightarrow} \\ \overset{R}{\Leftarrow} \end{array} \right\} \cdots \left\{ \begin{array}{c} \overset{R}{\Rightarrow} \\ \overset{R}{\Leftarrow} \end{array} \right\} \varphi_n$$

Obviamente, para cualquier sistema R, la relación de similaridad es de equivalencia.

Los sistemas de rescritura pueden emplearse para describir teorías lógicas ecuacionales, es decir, teorías en las que solamente se considera el predicado de igualdad y las fórmulas en forma prenexa están cuantificadas universalmente. Entonces, la relación de similaridad expresa el significado de la igualdad en la teoría lógica.

Más concretamente, sea una regla r de la forma $izq \Rightarrow der$. Notaremos por $\forall\vec{X}\varphi$ la clausura universal de φ. Llamemos $\Sigma(r)$ a la fórmula $\forall\vec{X} izq = der$ y $\Sigma(R)$ a la teoría $\{\Sigma(r) | r \in R\}$. Entonces tenemos la siguiente

Proposición 2.13 (Teorema de Birkhoff) *Sea R un sistema de rescritura. Sean t, s dos términos cualesquiera. Entonces, t y s son similares si y sólo si $\Sigma(R) \vDash \forall\vec{X} t = s$.*

DEMOSTRACIÓN: La dirección "si" es fácilmente demostrable, ya que si $t \overset{r}{\Rightarrow} s$, entonces $\Sigma(r) \vDash \forall\vec{X} t = s$, y también si $s \overset{r}{\Rightarrow} t$, entonces $\Sigma(r) \vDash \forall\vec{X} t = s$ (en ambos casos lo que hemos aplicado una versión restringida de la regla de paramodulación). Para la parte "sólo si", bastará comprobar que (i) si $s = t$ se deduce por paramodulación de $s_1(u) = t_1$ y $s_2 = t_2$, entonces s y t son similares según $\{r_1, r_2\}$, siendo r_1: $s_1 \Rightarrow t_1$ y r_2: $s_2 \Rightarrow t_2$; y (ii) si $s \overset{R}{\Leftrightarrow} t$, entonces para toda sustitución τ, $s\tau \overset{R}{\Leftrightarrow} t\tau$. Para (i), considérese que si $s = t$ se deduce por paramodulación, será por ejemplo de la forma $s_1\sigma[t_2\sigma] = t_1\sigma$, siendo $u\sigma = s_2\sigma$. Entonces $s_1\sigma[u\sigma] \overset{r_1}{\Rightarrow} t_1\sigma$ y $s_1\sigma[u\sigma] \overset{r_2}{\Rightarrow} s_1\sigma[t_2\sigma]$, o sea, $s_1\sigma[t_2\sigma] \overset{\{r_1,r_2\}}{\Leftrightarrow} t_1\sigma$. Para (ii), aplíquese τ a ambos miembros de la rescritura. Ahora bien, si $\Sigma(R) \vDash \forall\vec{X} t = s$, existe una derivación por resolución y paramodulación de la clásula vacía a partir de $\Sigma(R) \cup \{\mathsf{X} = \mathsf{X}\}$ (teorema 2.6), lo que en un teoría puramente ecuacional equivale a decir que existe una derivación por paramodulación de $\forall\vec{X} t' = s'$ a partir de $\Sigma(R) \cup \{\mathsf{X} = \mathsf{X}\}$ (siendo $t' = s'$ unificable con una instancia skolemizada de $t = s$) lo que por (ii) significa que t es similar a s. $\triangleleft$

Ejemplo 2.11 Consideremos los términos algebraicos en la notación habitual, generados por las constantes $\mathsf{a}, \mathsf{b}, \mathsf{c}, \ldots$, las variables $\mathsf{x}, \mathsf{y}, \ldots$ y las operaciones suma, resta, multiplicación y exponenciación. Sea el término

$t_1 = 5 \times \exp(\mathsf{a}, 0 \times x) + 0 \times \mathsf{b}$

y el sistema R_1

$$\begin{array}{ll} 0 \times \mathsf{X} \Rightarrow 0 & \mathsf{X} \times 0 \Rightarrow 0 \\ 1 \times \mathsf{X} \Rightarrow \mathsf{X} & \mathsf{X} \times 1 \Rightarrow \mathsf{X} \\ \exp(\mathsf{X}, 0) \Rightarrow 1 & \exp(0, \mathsf{X}) \Rightarrow 0 \\ 0 + \mathsf{X} \Rightarrow 0 & \mathsf{X} + 0 \Rightarrow 0 \end{array}$$

Entonces

$t_1 \overset{R_1}{\Rightarrow} 5 \times \exp(\mathsf{a}, 0 \times x) + 0$

y también, por ejemplo,

$t_1 \overset{R_1}{\Rightarrow} 5 \times \exp(\mathsf{a}, 0) + 0 \times \mathsf{b}$

En dos pasos tendremos, por ejemplo,

$t_1 \overset{R_1^*}{\Rightarrow} 5 \times \exp(\mathsf{a}, 0) + 0$

y finalmente

$t_1 \overset{R_1^*}{\Rightarrow} 5$

que ya no se puede rescribir más. Por otra parte será

$1 \times 5 \overset{R_1}{\Leftrightarrow} t_1$

ya que $1 \times 5 \Rightarrow 5$ y $t_1 \overset{R_1^*}{\Rightarrow} 5$. $\triangleleft$

Puede comprobarse que en el ejemplo anterior todas las cadenas de rescrituras terminan, y precisamente en este mismo término 5. Existen nombres especiales para estas deseables propiedades:

Definición 2.22 *Sea un sistema de rescritura R. Se dice que R* termina *(o que tiene la propiedad de terminación, o que es* noetheriano*) cuando no existe una sucesión infinita $(\varphi_1, \varphi_2, \ldots, \varphi_n, \ldots)$ tal que para todo par de elementos consecutivos se tiene que $\varphi_i \overset{R}{\Rightarrow} \varphi_{i+1}$.*

En algún caso, es fácil ver que un sistema no termina; por ejemplo, si contiene a la vez las dos reglas $t_1 \Rightarrow t_2$ y $t_2 \Rightarrow t_1$. Pero, en general, el problema de la terminación de un sistema de rescritura es indecidible (es posible describir los cálculos de una máquina de Turing mediante un sistema de rescritura y por tanto es posible reducir el problema de la parada al problema de la terminación de un sistema de rescritura). Ello no significa que no sea posible demostrar la terminación en muchos casos, basándose, por ejemplo, en la proposición 2.14.

Definición 2.23 *Consideremos un conjunto de términos $Term(\Omega)$ y sea $\prec$ una relación binaria bien fundamentada (vd. definición ??). Se dice que $\prec$ es monótona si para todos los términos s, t, u si $s \succ t$ entonces se tiene que $u[s] \succ u[t]$. Se dice que $\prec$ es plenamente invariante si para todos términos s, t y todas las sustituciones σ, si $s \succ t$ entonces se tiene que $s\sigma \succ t\sigma$. Se dice que $\prec$ es compatible con una regla $izq \Rightarrow der$ si $izq \succ der$.*

Proposición 2.14 *Sea un sistema de rescritura R. Si existe una relación binaria $\prec$ monótona, plenamente invariante y compatible con todas las reglas de R, entonces R termina.*

DEMOSTRACIÓN: Sea un término $t[l]$. Supongamos que se rescribe aplicando la regla r, $izq \Rightarrow der$. Entonces existe una sustitución σ tal que l coincide con $izq\sigma$ y la rescritura es $t[l] \overset{r}{\Rightarrow} t[der\sigma]$. Es fácil comprobar que $t[l] \succ t[der\sigma]$; en efecto, por ser $\prec$ compatible es $izq \succ der$, luego por ser plenamente invariante es $izq\sigma \succ der\sigma$, luego por ser monótona es $t[izq\sigma] \succ t[der\sigma]$. Hemos probado por tanto que en cada derivación los términos obtenidos son estrictamente decrecientes según $\prec$; y como $\prec$ está bien fundamentada, no podrán existir derivaciones infinitas. $\triangleleft$

La proposición anterior no dice cómo, dado un sistema R, se ha de construir una relación $\prec$ que cumpla las propiedades deseadas; de hecho, por la indecidibilidad antes mencionada, no puede haber un algoritmo que nos diga si tal relación existe o no.

Ejercicio 2.20 Consideremos la relación $t_1 \prec t_2$ definida como "la longitud de t_1 es menor que la longitud de t_2"

- Demostrar que $\prec$ es monótona, pero no es plenamente invariante.
- Sea el sistema R dado por las dos reglas
  $\mathsf{g(X,Y,Z)} \Rightarrow \mathsf{f(Z,Z)}$,
  $\mathsf{f(g(X,Y,Z),g(X,Y,Z))} \Rightarrow \mathsf{g(X,Y,g(X,Y,Z))}$.
  Demostrar que $\prec$ es compatible con R.
- Estudiar si R termina. (Pista: partir del término $\mathsf{g(a,b,g(a,b,c))}$.)

$\triangleleft$

Ejercicio 2.21 Consideremos la relación $t_1 \prec t_2$ definida como "t_1 es un subtérmino propio de t_2"

- Demostrar que $\prec$ es monótona y plenamente invariante.
- Sea el sistema R dado por la única regla $\mathsf{g(X,f(Y))} \Rightarrow \mathsf{f(Y)}$. Estudiar si R termina.

$\triangleleft$

Definición 2.24 *Sea un sistema R y sea t un término. Se dice que s es una forma normal de t cuando s cumple estas dos propiedades: i) $t \overset{R^*}{\Rightarrow} s$; ii) no existe ningún u tal que $s \overset{R^*}{\Rightarrow} u$.*

Definición 2.25 *Sea un sistema R. Dos términos t, s son* combinables *cuando existe un u tal que $t \overset{R^*}{\Rightarrow} u$ y $s \overset{R^*}{\Rightarrow} u$.*

Definición 2.26 *Sea un sistema R. Un término u es* no ambiguo *cuando todo par de términos t, s tales que $u \overset{R}{\Leftrightarrow} t$ y $u \overset{R}{\Leftrightarrow} s$ son combinables.*

Definición 2.27 *Un sistema R se dice que es* confluente *cuando todo término es no ambiguo.*

Proposición 2.15 *R es confluente si y sólo si todo par de términos similares t, s es combinable.*

DEMOSTRACIÓN: Se omite. ◁

Proposición 2.16 *Hay un algoritmo que decide si dos términos cualesquiera t, s son similares en un sistema de rescritura R noetheriano y confluente.*

DEMOSTRACIÓN: Sean t, s dos términos cualesquiera. Llamemos $R(t), R(s)$ a los conjuntos de rescrituras de t y de s, respectivamente. Supongamos que t y s son similares. Si R confluente, por la proposición 2.16 han de tener una rescritura común, así que ha de ser $R(t) \cup R(s) \neq \varnothing$. Supongamos ahora que $R(t) \cup R(s) = \varnothing$. Entonces es obvio que t y s son similares. Por tanto, t y s son similares si y sólo si $R(t) \cup R(s) = \varnothing$. Pero R es noetheriano, así que podemos calcular en tiempo finito ambos conjuntos. ◁

Definición 2.28 *Un sistema R se dice que es* localmente confluente *cuando para todo par de términos t, s se tiene que, si existe un u tal que $u \overset{R}{\Rightarrow} t$ y $u \overset{R}{\Rightarrow} s$, entonces existe un v tal que $t \overset{R^*}{\Rightarrow} v$ y $s \overset{R^*}{\Rightarrow} v$.*

Proposición 2.17 (Lema de Newman.) *Si R es localmente confluente y noetheriano, entonces R es confluente.*

2.8. RAZONAMIENTO MATEMATICO: TEORÍA DE GRUPOS.

Muchas teorías matemáticas pueden formalizarse, al menos en parte, como teorías de primer orden con igualdad; por ejemplo, la teoría de conjuntos (axiomas de Gödel-Barnays-von Neumann, axiomas de Zermelo-Fraenkel) y las teorías de las diversas estructuras algebraicas. Desarrollamos a continuación la formalización de una de ellas: la teoría elemental de grupos.

2.8.1. ONTOLOGÍA Y LEYES DEL DOMINIO.

En el caso de las teorías matemáticas, los objetos, propiedades y relaciones que deben considerarse en la teoría vienen ya dados sin ninguna ambigüedad. Concretamente, en la teoría de grupos debemos considerar los diversos elementos de un cierto conjunto. Entre ellos hay un elemento distinguido: el elemento neutro. En principio no se considera ninguna propiedad específica; por tanto, la única que se debe tomar en consideración es la identidad. Por otra parte, en un grupo se define una operación binaria, que a partir de dos elementos devuelve un tercero producto de ambos, y una operación monaria, que a partir de un elemento devuelve su inverso.

Las leyes del dominio vienen dadas por los axiomas que definen el concepto de grupo. Un conjunto habitual de axiomas es el siguiente:

1. La operación de grupo está definida para todo par de elementos del conjunto, y produce un elemento que también pertenece al conjunto.

2. La operación del grupo es asociativa.

3. Existe un elemento neutro e tal que, al operar e con cualquier elemento X, tanto por la derecha como por la izquierda, se obtiene el mismo elemento X.

4. Todo elemento X tiene un elemento inverso tal que al operar X con su inverso, tanto por la derecha como por la izquierda, se obtiene el elemento neutro.

Este conjunto de axiomas no es independiente. Por ejemplo, se puede suprimir la exigencia de neutro por la derecha, ya que se deduce de los restantes axiomas. Sin embargo, por simplificar los ejemplos, partiremos del conjunto de axiomas así enunciados

2.8.2. LENGUAJE Y AXIOMAS EN UN $CP^{=}$.

Necesitaremos una constante e para denotar al elemento neutro. Asimismo, necesitaremos un funtor binario prod(X, Y) para la operación del grupo. Siguiendo la notación habitual, lo escribiremos de forma infija (X . Y). También necesitamos un funtor unitario i(X) para simbolizar el elemento inverso. En este lenguaje los axiomas de grupo serán los de la tabla 2.3.

1.	$\forall X \forall Y \forall Z\ (X.(Y.Z)) = ((X.Y).Z)$	asociatividad
2.	$\forall X (X.e) = X$	neutro por la derecha
3.	$\forall X (e.X) = X$	neutro por la izquierda
4.	$\forall X (X.i(X)) = e$	inverso por la derecha
5.	$\forall X (i(X).X) = e$	inverso por la izquierda

Cuadro 2.3: Axiomas propios de la teoría de grupos.

Quizás el lector eche en falta un axioma que simbolice uno de los enunciados anteriores: "la operación de grupo está definida para todo par de elementos del conjunto, y produce un elemento que también pertenece al conjunto". Pero recuérdese lo dicho en 1.3.4 acerca de los funtores lógicos: la aplicación de un funtor a sus argumentos produce un término que para la semántica del CP siempre "existe", es decir, que en toda interpretación debe corresponder a "algo", precisamente a un elemento del dominio.

Los axiomas de la tabla 2.3 están ya en forma clausal. Los axiomas de igualdad de la teoría, en forma clausal, serán los de la tabla 2.4.

6.	$X = X$
7.	$\neg X = Y \vee Y = X$
8.	$\neg X = Y \vee \neg Y = Z \vee X = Z$
9.	$\neg X = Y \vee i(X) = i(Y)$
10.	$\neg X = Y \vee (X.Z) = (Y.Z)$
11.	$\neg X = Y \vee (Z.X) = (Z.Y)$

Cuadro 2.4: Axiomas de la igualdad en la teoría de grupos.

2.8.3. RAZONAMIENTO AUTOMÁTICO EN LA TEORÍA DE GRUPOS.

Demostremos ahora por los métodos estudiados algunos resultados elementales de la teoría de grupos. Empezaremos empleando el método de resolución y unificación manejando explícitamente los axiomas de la igualdad. Por tanto, partiremos del conjunto de cláusulas 1-11 de las tablas 2.3 y 2.4.

Razonamiento por resolución.

Probemos como ejemplo el siguiente teorema: *Hay un único elemento neutro a la izquierda.* Sea $\mathsf{neutroiz(X)}$ la fórmula abierta que simbolice *X es neutro por la izquierda.* Como sabemos, la existencia única se simbolizaría como

$$\exists \mathsf{X}(\mathsf{neutroiz(X)} \wedge \forall \mathsf{Y}(\mathsf{neutroiz(Y)} \rightarrow \mathsf{X} = \mathsf{Y}))$$

cuya negación es

$$\forall \mathsf{X}(\neg \mathsf{neutroiz(X)} \vee \exists \mathsf{Y}(\mathsf{neutroiz(Y)} \wedge \neg \mathsf{X} = \mathsf{Y})).$$

Pero $\mathsf{neutroiz(Z)}$ se define como $\forall \mathsf{Y}(\mathsf{Z}.\mathsf{Y}) = \mathsf{Y}$, y la fórmula completa será

$$\forall \mathsf{X}(\neg \forall \mathsf{Z}(\mathsf{X}.\mathsf{Z}) = \mathsf{Z} \vee \exists \mathsf{Y}(\forall \mathsf{Z}(\mathsf{Y}.\mathsf{Z}) = \mathsf{Z} \wedge \neg \mathsf{X} = \mathsf{Y})).$$

que skolemizada y en forma clausal queda

12. $\neg(\mathsf{X}.\mathsf{f}(\mathsf{X})) = \mathsf{f}(\mathsf{X}) \vee \mathsf{g}(\mathsf{X}).\mathsf{Z} = \mathsf{Z}$
13. $\neg(\mathsf{X}.\mathsf{f}(\mathsf{X})) = \mathsf{f}(\mathsf{X}) \vee \neg \mathsf{X} = \mathsf{g}(\mathsf{X})$

El conjunto inicial de cláusulas estará formado por los axiomas propios (1-5), los axiomas de la igualdad para esta teoría (6-11) y la negación del objetivo (12-13). Aplicando resolución obtenemos la prueba en 7 pasos de la tabla 2.5.

14.	$(\mathsf{g}(\mathsf{e}).\mathsf{Z}) = \mathsf{Z}$	de 12, 3
15.	$\mathsf{Z} = (\mathsf{g}(\mathsf{e}).\mathsf{Z})$	de 14, 7
16.	$\neg \mathsf{X} = (\mathsf{U}.\mathsf{e}) \vee \mathsf{X} = \mathsf{U}$	de 2 (segundo literal), 8
17.	$\mathsf{e} = \mathsf{g}(\mathsf{e})$	de 16, 15
18.	$\neg(\mathsf{e}.\mathsf{f}(\mathsf{e})) = \mathsf{f}(\mathsf{e})$	de 17, 13
19.	$\square$	de 18, 3

Cuadro 2.5: Demostración por resolución en la teoría de grupos.

Razonamiento por paramodulación.

Probemos el siguiente teorema: *Existe a lo sumo una solución de la ecuación* $a.X = b$ o, dicho más explícitamente, *para todos los elementos* a, b, c, d *del grupo, si* $a.c = b$ *y* $a.d = b$*, entonces* $c = d$. El objetivo es

$$\forall \mathsf{X} \forall \mathsf{Y} \forall \mathsf{Z}\,((\mathsf{X}.\mathsf{Y}) = (\mathsf{X}.\mathsf{Z}) \rightarrow \mathsf{Y} = \mathsf{Z})$$

que negado se convierte en

$$\exists \mathsf{X} \exists \mathsf{Y} \exists \mathsf{Z}((\mathsf{X}.\mathsf{Y}) = (\mathsf{X}.\mathsf{Z}) \wedge \neg \mathsf{Y} = \mathsf{Z}) \exists \mathsf{X} \exists \mathsf{Y} \exists \mathsf{Z}\,((\mathsf{X}.\mathsf{Y}) = (\mathsf{X}.\mathsf{Z}) \wedge \neg \mathsf{Y} = \mathsf{Z})$$

y skolemizado y en forma clausal queda

20. $(\mathsf{a}.\mathsf{b}) = (\mathsf{a}.\mathsf{c})$
21. $\neg \mathsf{b} = \mathsf{c}$

El conjunto inicial de cláusulas estará formado por los axiomas propios (1-5), el axioma reflexivo (6) y el objetivo negado (20-21). Aplicando resolución y paramodulación obtenemos la prueba en 7 pasos de la tabla 2.6. Empleando puramente resolución, la prueba más corta que los autores han podido encontrar consta de 16 pasos.

22.	$((\mathsf{X}.\mathsf{a}).\mathsf{b}) = (\mathsf{X}.(\mathsf{a}.\mathsf{c}))$	(param. 20 y 1)
23.	$(\mathsf{e}.\mathsf{b}) = (\mathsf{i}(\mathsf{a}).(\mathsf{a}.\mathsf{c}))$	(param. 22 y 5)
24.	$\mathsf{b} = (\mathsf{i}(\mathsf{a}).(\mathsf{a}.\mathsf{c}))$	(param. 23 y 3)
25.	$\mathsf{b} = ((\mathsf{i}(\mathsf{a}).\mathsf{a}).\mathsf{c})$	(param. 14 y 1)
26.	$\mathsf{b} = (\mathsf{e}.\mathsf{c})$	(param. 25 y 5)
27.	$\mathsf{b} = \mathsf{c}$	(param. 26 y 3)
28.	$\square$	(res. 27 y 21)

Cuadro 2.6: Demostración por paramodulación en la teoría de grupos.

Ejercicio 2.22 Un elemento de un grupo se dice autoinverso si operado consigo mismo produce el neutro. Simbolizar la siguiente proposición de la teoría de grupos y probarla mediante resolución y paramodulación: *Si todo elemento de un grupo es autoinverso, entonces el grupo es abeliano.*

Pistas: a) hallar una demostración en lenguaje natural e intentar expresarla mediante paramodulación; o mejor b) emplear un programa de demostración automática. $\triangleleft$

Limitaciones del lenguaje presentado.

Debemos señalar que la potencia expresiva de este lenguaje lógico no basta para representar todos los conceptos que aparecen en la teoría elemental de grupos. Consideremos por ejemplo la definición de *grupo de torsión*: se dice que un grupo es de torsión cuando todo elemento X del grupo es tal que operado consigo mismo un número finito de veces produce el elemento neutro. Si intentamos formalizar esta definición obtendremos algo así como

$$\forall \mathsf{X}(\mathsf{X} = \mathsf{e} \vee (\mathsf{X}.\mathsf{X}) = \mathsf{e} \vee (\mathsf{X}.(\mathsf{X}.\mathsf{X})) = \mathsf{e} \vee (\mathsf{X}.(\mathsf{X}.(\mathsf{X}.\mathsf{X})) = \mathsf{e} \vee \ldots)$$

que no es una cadena finita de símbolos. Otra alternativa sería definir la operación binaria de exponenciación X^n, y escribir la fórmula $\forall \mathsf{X} \exists \mathsf{N}\ \mathsf{exp}(\mathsf{X}, \mathsf{N}) = \mathsf{e}$; pero nótese que para ello tendremos que formalizar también la aritmética de los números naturales, lo que se sale claramente de las posibilidades del lenguaje propuesto en esta sección.