```
#|

 Copyright (C) 1994 by Yuan Yu.  All Rights Reserved.

 This script is hereby placed in the public domain, and therefore unlimited
 editing and redistribution is permitted.

 NO WARRANTY

 Yuan Yu PROVIDES ABSOLUTELY NO WARRANTY.  THE EVENT SCRIPT IS PROVIDED "AS IS"
 WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT
 LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
 PARTICULAR PURPOSE.  THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE
 SCRIPT IS WITH YOU.  SHOULD THE SCRIPT PROVE DEFECTIVE, YOU ASSUME THE COST OF
 ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

 IN NO EVENT WILL Yuan Yu BE LIABLE TO YOU FOR ANY DAMAGES, ANY LOST PROFITS,
 LOST MONIES, OR OTHER SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT
 OF THE USE OR INABILITY TO USE THIS SCRIPT (INCLUDING BUT NOT LIMITED TO LOSS
 OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY THIRD
 PARTIES), EVEN IF YOU HAVE ADVISED US OF THE POSSIBILITY OF SUCH DAMAGES, OR
 FOR ANY CLAIM BY ANY OTHER PARTY.

|#

; Requires defn-sk.

#|
The following article is about this event file.

@article{Yu89,
        author="Yuan Yu",
        title="Computer Proofs in Group Theory",
        journal="Journal of Automated Reasoning",
        volume="6",
number="3",
        year=1990
}
|#
```

Event: Start with the initial **thm** theory.

```
; First, several concepts on SET.

; Set L has no duplicate element.
```

DEFINITION:
set-standard (l)
$=$ **if** listp (l) **then** $(\mathrm{car}(l) \notin \mathrm{cdr}(l)) \wedge$ set-standard $(\mathrm{cdr}(l))$
else t endif

```
; L1-L2.
```

DEFINITION:
set-minus $(l1, l2)$
$=$ **if** listp $(l1)$
then if $\mathrm{car}(l1) \in l2$ **then** set-minus $(\mathrm{cdr}(l1), l2)$
else cons $(\mathrm{car}(l1)$, set-minus $(\mathrm{cdr}(l1), l2))$ **endif**
else $l1$ **endif**

```
; L1 and L2 are disjoint.
```

DEFINITION:
set-disjoint $(l1, l2)$
$=$ **if** listp $(l1)$
then if $\mathrm{car}(l1) \in l2$ **then f**
else set-disjoint $(\mathrm{cdr}(l1), l2)$ **endif**
else t endif

```
; remove the element x from L.
```

DEFINITION:
delete (x, l)
$=$ **if** listp (l)
then if $x = \mathrm{car}(l)$ **then** $\mathrm{cdr}(l)$
else cons $(\mathrm{car}(l)$, delete $(x, \mathrm{cdr}(l)))$ **endif**
else l **endif**

```
; L2 contains L1.
```

DEFINITION:
subset $(l1, l2)$
$=$ **if** listp $(l1)$ **then** $(\mathrm{car}(l1) \in l2) \wedge$ subset $(\mathrm{cdr}(l1), l2)$
else t endif

```
; The number of elements in L.
```

DEFINITION:
cardinal (l)
$=$ **if** listp (l) **then** $1 +$ cardinal (cdr (l))
else `0` **endif**

```
; Lemmas based on the above concepts.
```

THEOREM: set-standard-lemma
set-standard $(a) \rightarrow$ set-standard (set-minus (a, b))

THEOREM: set-minus-lemma1
count (set-minus $(s, s1)$) $\leq$ count (s)

THEOREM: set-minus-lemma2
$(c \notin a) \rightarrow$ (set-minus $(a$, cons $(c, b))$ = set-minus (a, b))

THEOREM: set-minus-lemma3
$(x \in$ set-minus $(s, s1)) = ((x \in s) \wedge (x \notin s1))$

THEOREM: set-minus-lemma
(listp $(s) \wedge (x \in s) \wedge (x \in s1)$)
$\rightarrow$ (count (set-minus $(s, s1)$) $<$ count (s))

THEOREM: delete-lemma1
$(x \in a) \rightarrow$ (cardinal $(a) = (1 +$ cardinal (delete (x, a))))

THEOREM: delete-lemma2
$((y \in a) \wedge (x \neq y)) \rightarrow (y \in$ delete $(x, a))$

THEOREM: delete-lemma3
$((x \in a) \wedge (x \notin b) \wedge$ subset $(b, a)) \rightarrow$ subset $(b$, delete $(x, a))$

THEOREM: subset-transitivity
(subset $(a, b) \wedge$ subset $(b, c)) \rightarrow$ subset (a, c)

THEOREM: subset-lemma0
(subset $(s1, s) \wedge (x \in s1)) \rightarrow (x \in s)$

THEOREM: subset-lemma1
subset $(a, b) \rightarrow$ subset $(a$, cons $(c, b))$

THEOREM: subset-lemma2
subset $(a, b) \rightarrow$ subset (set-minus $(a, c), b)$

THEOREM: subset-reflexivity
subset (a, a)

THEOREM: cardinal-lemma
$(x \in s) \rightarrow (1 \leq \text{cardinal}(s))$

THEOREM: cardinal-equality
$(\text{set-standard}(a) \wedge (c \notin b) \wedge (c \in a))$
$\rightarrow \quad (\text{cardinal}(\text{set-minus}(a, b)) = (1 + \text{cardinal}(\text{set-minus}(a, \text{cons}(c, b)))))$

```
; Induction hint for CARDINAL-INEQUALITY-LEMMA
```

DEFINITION:
cardinal-inequality-induct (b, a)
= **if** listp (b) **then** cardinal-inequality-induct (cdr (b), delete (car (b), a))
else t endif

THEOREM: cardinal-inequality
$(\text{set-standard}(b) \wedge \text{subset}(b, a)) \rightarrow (\text{cardinal}(b) \leq \text{cardinal}(a))$

THEOREM: cardinal-subset
$(\text{set-standard}(a) \wedge \text{set-standard}(b) \wedge \text{subset}(b, a))$
$\rightarrow \quad (\text{cardinal}(\text{set-minus}(a, b)) = (\text{cardinal}(a) - \text{cardinal}(b)))$

```
; we will introduce the axioms for definition of group with operation OP.
```

EVENT: Introduce the function symbol *op* of 2 arguments.

DEFINITION:
group-op (g)

$$
\begin{aligned}
\leftrightarrow \quad & (\forall\, x, y\ (((x \in g) \wedge (y \in g)) \rightarrow (\text{op}(x, y) \in g)) \\
& \wedge\ \forall\, x, y, z\ (((x \in g) \wedge (y \in g) \wedge (z \in g)) \\
& \qquad \rightarrow (\text{op}(\text{op}(x, y), z) = \text{op}(x, \text{op}(y, z)))) \\
& \wedge\ \exists\, id\ ((id \in g) \\
& \qquad \wedge\ \forall\, x\ ((x \in g) \\
& \qquad\qquad \rightarrow ((\text{op}(id, x) = x) \\
& \qquad\qquad\quad \wedge\ (\text{op}(x, id) = x) \\
& \qquad\qquad\quad \wedge\ \exists\, inv\ ((inv \in g) \\
& \qquad\qquad\qquad \wedge\ (\text{op}(inv, x) = id) \\
& \qquad\qquad\qquad \wedge\ (\text{op}(x, inv) = id))))))
\end{aligned}
$$

```
; the group has the "closed" property.
```

THEOREM: group-op-closed
$(\text{group-op}(g) \wedge (x \in g) \wedge (y \in g)) \rightarrow (\text{op}(x, y) \in g)$

```
; the group has the "associativity" property.
```

THEOREM: group-op-associativity
$(\text{group-op}(g) \land (x \in g) \land (y \in g) \land (z \in g))$
$\rightarrow \quad (\text{op}(\text{op}(x,\ y),\ z) = \text{op}(x,\ \text{op}(y,\ z)))$

THEOREM: group-op-associativity1
$(\text{group-op}(g) \land (x \in g) \land (y \in g) \land (z \in g))$
$\rightarrow \quad (\text{op}(x,\ \text{op}(y,\ z)) = \text{op}(\text{op}(x,\ y),\ z))$

```
; the group has the "identity" property.
```

THEOREM: group-op-identity
$\text{group-op}(g)$
$\rightarrow \quad ((\text{id}(g) \in g)$
$\quad \land \quad ((x \in g) \rightarrow ((\text{op}(\text{id}(g),\ x) = x) \land (\text{op}(x,\ \text{id}(g)) = x))))$

```
; the group has the "inverse" property.
```

THEOREM: group-op-inverse
$(\text{group-op}(g) \land (x \in g))$
$\rightarrow \quad ((\text{inv}(g,\ x) \in g)$
$\quad \land \quad (\text{op}(\text{inv}(g,\ x),\ x) = \text{id}(g))$
$\quad \land \quad (\text{op}(x,\ \text{inv}(g,\ x)) = \text{id}(g)))$

```
; introduce the concept of coset.
```

DEFINITION:
$\text{right-coset}(s,\ a)$
$= \quad$ **if** $\text{listp}(s)$ **then** $\text{cons}(\text{op}(\text{car}(s),\ a),\ \text{right-coset}(\text{cdr}(s),\ a))$
else nil endif

THEOREM: right-coset-cardinal
$\text{cardinal}(\text{right-coset}(s,\ a)) = \text{cardinal}(s)$

THEOREM: right-coset-nempty
$(\text{group-op}(g) \land (x \in g) \land \text{subset}(s,\ g) \land (\text{id}(g) \in s))$
$\rightarrow \quad (x \in \text{right-coset}(s,\ x))$

```
; some simple equalities in group.
; EQUALITY1: x*a=y*b-->x=y*(b*(inv g a)).
```

THEOREM: op-equality1
$(\text{group-op}(g)$
$\land \quad (x \in g)$
$\land \quad (y \in g)$
$\land \quad (a \in g)$
$\land \quad (b \in g)$
$\land \quad (\text{op}(x,\ a) = \text{op}(y,\ b)))$
$\rightarrow \quad (x = \text{op}(y,\ \text{op}(b,\ \text{inv}(g,\ a))))$

```
; EQUALITY2: x*a=y*b-->a=((inv g x)*y)*b.
```

THEOREM: op-equality2
(group-op (g)
 $\wedge$ $(x \in g)$
 $\wedge$ $(y \in g)$
 $\wedge$ $(a \in g)$
 $\wedge$ $(b \in g)$
 $\wedge$ $(\text{op}\,(x,\ a) = \text{op}\,(y,\ b)))$
$\rightarrow$ $(a = \text{op}\,(\text{op}\,(\text{inv}\,(g,\ x),\ y),\ b))$

```
; cancellation: xa=ya-->x=y.
```

THEOREM: cancellation
(group-op (g)
 $\wedge$ $(x \in g)$
 $\wedge$ $(y \in g)$
 $\wedge$ $(a \in g)$
 $\wedge$ $(\text{op}\,(x,\ a) = \text{op}\,(y,\ a)))$
$\rightarrow$ $(x = y)$

```
; some further simple equalities.
```

THEOREM: op-equality3
(group-op $(g) \wedge (x \in g) \wedge (a \in g) \wedge (\text{op}\,(x,\ a) = \text{id}\,(g)))$
$\rightarrow$ $(a = \text{inv}\,(g,\ x))$

THEOREM: op-equality4
(group-op $(g) \wedge (x \in g) \wedge (\text{op}\,(x,\ x) = x)) \rightarrow (x = \text{id}\,(g))$

DEFINITION:
subgroup-op $(h,\ g) =$ (group-op $(g) \wedge$ group-op $(h) \wedge$ subset $(h,\ g))$

```
; (id g)=(id h), if h is a subgroup of g.
```

THEOREM: op-identity-same
subgroup-op $(h,\ g) \rightarrow (\text{id}\,(g) = \text{id}\,(h))$

THEOREM: op-identity-in-subgroup
subgroup-op $(h,\ g) \rightarrow (\text{id}\,(g) \in h)$

```
; (inv g x)=(inv h x), if h is a subgroup of g.
```

THEOREM: op-inverse-same
(subgroup-op $(h,\ g) \wedge (x \in h)) \rightarrow (\text{inv}\,(h,\ x) = \text{inv}\,(g,\ x))$

THEOREM: op-inverse-in-subgroup
$(\text{subgroup-op}(h, g) \land (x \in h)) \rightarrow (\text{inv}(g, x) \in h)$

THEOREM: group-op-order
$\text{group-op}(g) \rightarrow (1 \leq \text{cardinal}(g))$

EVENT: Disable group-op.

EVENT: Disable group-op-associativity1.

```
; we will introduce the axioms for another group with operation OP1.
```

EVENT: Introduce the function symbol *op1* of 2 arguments.

DEFINITION:
group-op1 (h)

$$
\begin{aligned}
\leftrightarrow \quad & (\forall\, x, y\, (((x \in h) \land (y \in h)) \rightarrow (\text{op1}(x, y) \in h)) \\
& \land \quad \forall\, x, y, z\, (((x \in h) \land (y \in h) \land (z \in h)) \\
& \qquad\qquad \rightarrow \quad (\text{op1}(\text{op1}(x, y), z) = \text{op1}(x, \text{op1}(y, z)))) \\
& \land \quad \exists\, id\, ((id \in h) \\
& \qquad\quad \land \quad \forall\, x\, ((x \in h) \\
& \qquad\qquad\quad \rightarrow \quad ((\text{op1}(id, x) = x) \\
& \qquad\qquad\qquad \land \quad (\text{op1}(x, id) = x) \\
& \qquad\qquad\qquad \land \quad \exists\, inv\, ((inv \in h) \\
& \qquad\qquad\qquad\qquad \land \quad (\text{op1}(inv, x) = id) \\
& \qquad\qquad\qquad\qquad \land \quad (\text{op1}(x, inv) = id))))))
\end{aligned}
$$

```
; the group has the "closed" property.
```

THEOREM: group-op1-closed
$(\text{group-op1}(h) \land (x \in h) \land (y \in h)) \rightarrow (\text{op1}(x, y) \in h)$

```
; the group has the "associativity" property.
```

THEOREM: group-op1-associativity
$(\text{group-op1}(h) \land (x \in h) \land (y \in h) \land (z \in h))$
$\rightarrow \quad (\text{op1}(\text{op1}(x, y), z) = \text{op1}(x, \text{op1}(y, z)))$

THEOREM: group-op1-associativity1
$(\text{group-op1}(h) \land (x \in h) \land (y \in h) \land (z \in h))$
$\rightarrow \quad (\text{op1}(x, \text{op1}(y, z)) = \text{op1}(\text{op1}(x, y), z))$

```
; the group has the "identity" property.
```

THEOREM: group-op1-identity

$$
\begin{aligned}
&\text{group-op1}(h)\\
\rightarrow\ &((\text{id-1}(h) \in h)\\
&\quad \wedge\ ((x \in h)\\
&\qquad \rightarrow\ ((\text{op1}(\text{id-1}(h),\, x) = x) \wedge (\text{op1}(x,\, \text{id-1}(h)) = x))))
\end{aligned}
$$

```
; the group has the "inverse" property.
```

THEOREM: group-op1-inverse

$$
\begin{aligned}
&(\text{group-op1}(h) \wedge (x \in h))\\
\rightarrow\ &((\text{inv-1}(h,\, x) \in h)\\
&\quad \wedge\ (\text{op1}(\text{inv-1}(h,\, x),\, x) = \text{id-1}(h))\\
&\quad \wedge\ (\text{op1}(x,\, \text{inv-1}(h,\, x)) = \text{id-1}(h)))
\end{aligned}
$$

```
; some simple equalities in group.
; OP1-EQUALITY1: x*a=y*b-->x=y*(b*(inv a)).
```

THEOREM: op1-equality1

$$
\begin{aligned}
&(\text{group-op1}(h)\\
&\ \wedge\ (x \in h)\\
&\ \wedge\ (y \in h)\\
&\ \wedge\ (a \in h)\\
&\ \wedge\ (b \in h)\\
&\ \wedge\ (\text{op1}(x,\, a) = \text{op1}(y,\, b)))\\
\rightarrow\ &(x = \text{op1}(y,\, \text{op1}(b,\, \text{inv-1}(h,\, a))))
\end{aligned}
$$

```
; EQUALITY2: x*a=y*b-->a=((inv x)*y)*b.
```

THEOREM: op1-equality2

$$
\begin{aligned}
&(\text{group-op1}(h)\\
&\ \wedge\ (x \in h)\\
&\ \wedge\ (y \in h)\\
&\ \wedge\ (a \in h)\\
&\ \wedge\ (b \in h)\\
&\ \wedge\ (\text{op1}(x,\, a) = \text{op1}(y,\, b)))\\
\rightarrow\ &(a = \text{op1}(\text{op1}(\text{inv-1}(h,\, x),\, y),\, b))
\end{aligned}
$$

THEOREM: op1-equality3

$$
\begin{aligned}
&(\text{group-op1}(h) \wedge (x \in h) \wedge (a \in h) \wedge (\text{op1}(x,\, a) = \text{id-1}(h)))\\
\rightarrow\ &(a = \text{inv-1}(h,\, x))
\end{aligned}
$$

THEOREM: op1-equality4

$$
(\text{group-op1}(h) \wedge (x \in h) \wedge (\text{op1}(x,\, x) = x)) \rightarrow (x = \text{id-1}(h))
$$

```
; cancellation: xa=ya-->x=y.
```

THEOREM: op1-cancellation
(group-op1 (h)
 $\land$ $(x \in h)$
 $\land$ $(y \in h)$
 $\land$ $(a \in h)$
 $\land$ (op1 $(x,\ a)$ = op1 $(y,\ a)$))
$\rightarrow$ $(x = y)$

```
; we start to prove the kernel of a group homomorphism is a normal subgroup.
; Introduce homomorphisms.
```

EVENT: Introduce the function symbol *phi* of one argument.

DEFINITION:
homo-phi $(g,\ h)$
$\leftrightarrow$ $\forall\ x,\ y$ $(((x \in g) \land (y \in g))$
 $\rightarrow$ ((phi $(x) \in h)$
 $\land$ (phi $(y) \in h)$
 $\land$ (phi (op $(x,\ y)$) = op1 (phi (x), phi (y))))))

THEOREM: homomorphism-phi
(homo-phi $(g,\ h) \land (x \in g) \land (y \in g)$)
$\rightarrow$ ((phi $(x) \in h)$
 $\land$ (phi $(y) \in h)$
 $\land$ (phi (op $(x,\ y)$) = op1 (phi (x), phi (y)))))

DEFINITION:
phi-inv $(g,\ a)$
= **if** listp (g)
 then if phi (car (g)) = a **then** cons (car (g), phi-inv (cdr (g), a))
 else phi-inv (cdr (g), a) **endif**
 else nil endif

THEOREM: basic-mapping1
$((x \in g) \land$ (phi $(x) = a)) \rightarrow (x \in$ phi-inv $(g,\ a))$

THEOREM: basic-mapping2
$(x \in$ phi-inv $(g,\ a)) \rightarrow$ (phi $(x) = a)$

THEOREM: phi-inv-subset
subset (phi-inv $(g,\ a),\ g)$

THEOREM: id-to-id
(group-op (g) $\land$ group-op1 (h) $\land$ homo-phi $(g,\ h)$)
$\rightarrow$ (phi (id (g)) = id-1 (h))

Theorem: inv-to-inv
$(\text{group-op}(g) \land \text{group-op1}(h) \land \text{homo-phi}(g, h) \land (x \in g))$
$\rightarrow \quad (\text{phi}(\text{inv}(g, x)) = \text{inv-1}(h, \text{phi}(x)))$

Theorem: ker-closed
$(\text{group-op}(g)$
$\land \quad \text{group-op1}(h)$
$\land \quad \text{homo-phi}(g, h)$
$\land \quad (x \in \text{phi-inv}(g, \text{id-1}(h)))$
$\land \quad (y \in \text{phi-inv}(g, \text{id-1}(h))))$
$\rightarrow \quad (\text{op}(x, y) \in \text{phi-inv}(g, \text{id-1}(h)))$

Theorem: ker-associativity
$(\text{group-op}(g)$
$\land \quad (x \in \text{phi-inv}(g, a))$
$\land \quad (y \in \text{phi-inv}(g, a))$
$\land \quad (z \in \text{phi-inv}(g, a)))$
$\rightarrow \quad (\text{op}(\text{op}(x, y), z) = \text{op}(x, \text{op}(y, z)))$

Theorem: ker-identity
$(\text{group-op}(g) \land \text{group-op1}(h) \land \text{homo-phi}(g, h))$
$\rightarrow \quad (\text{id}(g) \in \text{phi-inv}(g, \text{id-1}(h)))$

Theorem: id-inv-id
$\text{group-op1}(h) \rightarrow (\text{inv-1}(h, \text{id-1}(h)) = \text{id-1}(h))$

Theorem: ker-inverse
$(\text{group-op}(g)$
$\land \quad \text{group-op1}(h)$
$\land \quad \text{homo-phi}(g, h)$
$\land \quad (x \in \text{phi-inv}(g, \text{id-1}(h))))$
$\rightarrow \quad (\text{inv}(g, x) \in \text{phi-inv}(g, \text{id-1}(h)))$

Theorem: ker-identity-inverse
$(\text{group-op}(g) \land \text{group-op1}(h) \land \text{homo-phi}(g, h))$
$\rightarrow \quad ((x \in \text{phi-inv}(g, \text{id-1}(h)))$
$\quad \rightarrow \quad ((\text{op}(\text{id}(g), x) = x)$
$\quad\quad \land \quad (\text{op}(x, \text{id}(g)) = x)$
$\quad\quad \land \quad (\text{inv}(g, x) \in \text{phi-inv}(g, \text{id-1}(h)))$
$\quad\quad \land \quad (\text{op}(\text{inv}(g, x), x) = \text{id}(g))$
$\quad\quad \land \quad (\text{op}(x, \text{inv}(g, x)) = \text{id}(g))))$

Theorem: ker-subgroup
$(\text{group-op}(g) \land \text{group-op1}(h) \land \text{homo-phi}(g, h))$
$\rightarrow \quad \text{group-op}(\text{phi-inv}(g, \text{id-1}(h)))$

DEFINITION:
op-normalp $(g,\ n)$
$\leftrightarrow \quad \forall\, x,\ y\ (((x \in g) \land (y \in n)) \rightarrow (\mathrm{op}\,(\mathrm{op}\,(x,\ y),\ \mathrm{inv}\,(g,\ x)) \in n))$

DEFINITION:
normal-subgroup-op $(g,\ n)$
$= \quad$ (group-op (g) $\land$ group-op (n) $\land$ subset $(n,\ g)$ $\land$ op-normalp $(g,\ n)$)

THEOREM: normal-lemma
(group-op (g)
$\land$ group-op1 (h)
$\land$ homo-phi $(g,\ h)$
$\land$ $(x \in g)$
$\land$ $(y \in$ phi-inv $(g,$ id-1 $(h))))$
$\rightarrow$ (op (op $(x,\ y)$, inv $(g,\ x)) \in$ phi-inv $(g,$ id-1 $(h)))$

THEOREM: ker-normal
(group-op (g) $\land$ group-op1 (h) $\land$ homo-phi $(g,\ h)$)
$\rightarrow$ op-normalp $(g,$ phi-inv $(g,$ id-1 $(h)))$

THEOREM: ker-normal-subgroup
(group-op (g) $\land$ group-op1 (h) $\land$ homo-phi $(g,\ h)$)
$\rightarrow$ normal-subgroup-op $(g,$ phi-inv $(g,$ id-1 $(h)))$

EVENT: Enable group-op-associativity1.

```
; Now back to the proof of Lagrange Theorem.
; Every coset of s in a group is "set-standard".
```

THEOREM: right-coset-standard-1
(group-op (g) $\land$ subset $(s,\ g)$ $\land$ $(a \in g)$ $\land$ $(x \in g)$ $\land$ $(x \notin s)$)
$\rightarrow$ (op $(x,\ a) \notin$ right-coset $(s,\ a)$)

THEOREM: right-coset-standard-2
(group-op (g) $\land$ subset $(s,\ g)$ $\land$ set-standard (s) $\land$ $(a \in g)$)
$\rightarrow$ set-standard (right-coset $(s,\ a)$)

THEOREM: right-coset-standard
(subgroup-op $(h,\ g)$ $\land$ set-standard (h) $\land$ $(a \in g)$)
$\rightarrow$ set-standard (right-coset $(h,\ a)$)

```
; different cosets are disjoint.
```

THEOREM: right-coset-disjoint-lemma
(group-op (g)

$\wedge$ subset $(s,\ g)$
$\wedge$ $(x \in g)$
$\wedge$ $(y \in g)$
$\wedge$ $(a \in g)$
$\wedge$ $(b \in g)$
$\wedge$ $(\text{op}\,(\text{inv}\,(g,\ x),\ y) \in s)$
$\wedge$ $(a \notin \text{right-coset}\,(s,\ b)))$
$\rightarrow$ $(\text{op}\,(x,\ a) \neq \text{op}\,(y,\ b))$

Theorem: right-coset-disjoint-1
(subgroup-op $(h,\ g)$
$\wedge$ subset $(s,\ h)$
$\wedge$ $(x \in h)$
$\wedge$ $(a \in g)$
$\wedge$ $(b \in g)$
$\wedge$ $(a \notin \text{right-coset}\,(h,\ b)))$
$\rightarrow$ $(\text{op}\,(x,\ a) \notin \text{right-coset}\,(s,\ b))$

Theorem: right-coset-disjoint-2
(subgroup-op $(h,\ g)$
$\wedge$ $(x \in h)$
$\wedge$ $(a \in g)$
$\wedge$ $(b \in g)$
$\wedge$ $(a \notin \text{right-coset}\,(h,\ b)))$
$\rightarrow$ $(\text{op}\,(x,\ a) \notin \text{right-coset}\,(h,\ b))$

Theorem: right-coset-disjoint-3
(subgroup-op $(h,\ g)$
$\wedge$ subset $(s,\ h)$
$\wedge$ $(a \in g)$
$\wedge$ $(b \in g)$
$\wedge$ $(a \notin \text{right-coset}\,(h,\ b)))$
$\rightarrow$ set-disjoint (right-coset $(s,\ a)$, right-coset $(h,\ b)$)

Theorem: right-coset-disjoint
(subgroup-op $(h,\ g) \wedge (a \in g) \wedge (b \in g) \wedge (a \notin \text{right-coset}\,(h,\ b)))$
$\rightarrow$ set-disjoint (right-coset $(h,\ a)$, right-coset $(h,\ b)$)

```
; Now the Lagrange Theorem will be attacked.
; First, we still need some lemmas.
; first, disable GROUP.
```

Event: Disable group-op.

Definition:

op-closed $(s1,\ s2)$
$\leftrightarrow \quad \forall\, x,\ y\ (((x \in s1) \land (y \in s2)) \rightarrow (\text{op}\,(x,\ y) \in s2))$

THEOREM: la-lemma1
$((b \in s) \land \text{subset}\,(h1,\ h) \land \text{op-closed}\,(h,\ s))$
$\rightarrow \quad \text{subset}\,(\text{right-coset}\,(h1,\ b),\ s)$

THEOREM: la-lemma2
$(\text{subgroup-op}\,(h,\ g) \land \text{subset}\,(s,\ g) \land (b \in g) \land \text{op-closed}\,(h,\ s))$
$\rightarrow \quad (((x \in h) \land (a \in \text{set-minus}\,(s,\ \text{right-coset}\,(h,\ b))))$
$\qquad \rightarrow \quad (\text{op}\,(x,\ a) \in \text{set-minus}\,(s,\ \text{right-coset}\,(h,\ b))))$

THEOREM: la-lemma3
$(\text{subgroup-op}\,(h,\ g) \land \text{subset}\,(s,\ g) \land (b \in g) \land \text{op-closed}\,(h,\ s))$
$\rightarrow \quad \text{op-closed}\,(h, \text{set-minus}\,(s,\ \text{right-coset}\,(h,\ b)))$

THEOREM: lagrange-induct-measure
$(\text{group-op}\,(g) \land \text{group-op}\,(h) \land \text{subset}\,(h,\ g) \land \text{subset}\,(s,\ g) \land \text{listp}\,(s))$
$\rightarrow \quad (\text{count}\,(\text{set-minus}\,(s,\ \text{right-coset}\,(h,\ \text{car}\,(s)))) < \text{count}\,(s))$

THEOREM: la-lemma4
$((y \leq x) \land (1 \leq y) \land (((x - y)\ \textbf{mod}\ y) = 0))$
$\rightarrow \quad ((x\ \textbf{mod}\ y) = 0)$

THEOREM: la-lemma5
$(\text{subgroup-op}\,(h,\ g)$
$\land \quad \text{set-standard}\,(h)$
$\land \quad \text{subset}\,(s,\ g)$
$\land \quad \text{set-standard}\,(s)$
$\land \quad \text{op-closed}\,(h,\ s)$
$\land \quad ((\text{cardinal}\,(\text{set-minus}\,(s,\ \text{right-coset}\,(h,\ \text{car}\,(s))))\ \textbf{mod}\ \text{cardinal}\,(h))$
$\qquad = \quad 0))$
$\rightarrow \quad ((\text{cardinal}\,(s)\ \textbf{mod}\ \text{cardinal}\,(h)) = 0)$

DEFINITION:
lagrange-induct $(g,\ h,\ s)$
$= \quad$ **if** subgroup-op $(h,\ g) \land$ subset $(s,\ g) \land$ listp (s)
then lagrange-induct $(g,\ h,$ set-minus $(s,$ right-coset $(h,$ car $(s))))$
else t endif

THEOREM: lagrange-generalized
$(\text{subgroup-op}\,(h,\ g)$
$\land \quad \text{set-standard}\,(h)$
$\land \quad \text{subset}\,(s,\ g)$
$\land \quad \text{set-standard}\,(s)$
$\land \quad \text{op-closed}\,(h,\ s))$
$\rightarrow \quad ((\text{cardinal}\,(s)\ \textbf{mod}\ \text{cardinal}\,(h)) = 0)$

DEFINITION: $\text{divides}\,(m,\ n) = ((n\ \mathbf{mod}\ m) = \mathtt{0})$

THEOREM: subset-op-closed
$(\text{group-op}\,(g) \land \text{subset}\,(h,\ g)) \rightarrow \text{op-closed}\,(h,\ g)$

THEOREM: lagrange
$(\text{subgroup-op}\,(h,\ g) \land \text{set-standard}\,(g) \land \text{set-standard}\,(h))$
$\rightarrow \quad \text{divides}\,(\text{cardinal}\,(h),\ \text{cardinal}\,(g))$

Index