AXIOMATIQUE A UN AXIOME DONT LA THEORIE EST CELLE DES GROUPES ABELIENS

par: *Jean-Marie Huard*
Cegep du Vieux-Montréal.

Soit A un ensemble,
$*$ une opération dans A

axiome: Soit $a, b, c \in A$
$a = (b * ((b * c) * (a * c)))$

théorème 1: Soit $d, e, f \in A$
Si $(d * e) = (f * e)$ alors $d = f$

preuve:

(1)	$(d * e) = (f * e)$	(hypothèse)
(2)	$d = (e * ((e * e) * (d * e)))$	(axiome)
(3)	$d = (e * ((e * e) * (f * e)))$	(2) (1) (égalité)
(4)	$f = (e * ((e * e) * (f * e)))$	(axiome)
(5)	$d = f$	(3) (4) (égalité)

théorème 2: Soit $g, h, i \in A$
$((g * (h * i)) * i) = (g * h)$

preuve:

(1)	posons $j = (h * i)$	
(2)	posons $l = (g * j)$	
(3)	posons $k = (l * i)$	
(4)	$((g * j) * (k * j)) = (l * (k * j))$	(2) (égalité)
(5)	$(l * (k * j)) = (l * ((l * i) * (h * i)))$	(3)(1) (égalité)

(6)	$(l * ((l * i) * (h * i))) = h$	(axiome)
(7)	$((g * j) * (k * j)) = h$	(4) (5) (6) (ég.)
(8)	$k = (g * ((g * j) * (k * j)))$	(axiome)
(9)	$k = (g * h)$	(8) (7) (ég.)
(10)	$(l * i) = (g * h)$	(9) (3) (ég.)
(11)	$((g * j) * i) = (g * h)$	(10) (2) (ég.)
(12)	$((g * (h * i)) * i) = (g * h)$	(11) (1) (ég.)

théorème 3: Soit $m, n \in A$

$(m * (n * n)) = m$

preuve:

(1)	$((m * (n * n)) * n) = (m * n)$	(théorème 2)
(2)	$(m * (n * n)) = m$	(1) (théorème 1)

théorème 4: Soit $o, p \in A$

$o = (p * (p * o))$

preuve:

(1)	posons $q = (p * o)$	
(2)	$o = (p * ((p * o) * (o * o)))$	(axiome)
(3)	$o = (p * (q * (o * o)))$	(2) (1) (ég.)
(4)	$(q * (o * o)) = q$	(théorème 3)
(5)	$o = (p * q)$	(3) (4) (ég.)
(6)	$o = (p * (p * o))$	(5) (1) (ég.)

théorème 5: Soit $r, s, t \in A$

Si $(r * s) = (r * t)$ alors $s = t$

preuve:

(1)	$(r * s) = (r * t)$	(hypothèse)
(2)	$s = (r * (r * s))$	(théorème 4)
(3)	$s = (r * (r * t))$	(2) (1) (ég.)

(4)	$t = (r * (r * t))$	(théorème 4)
(5)	$s = t$	(3) (4) (ég.)

théorème 6: Soit $u, v \in A$

$(u * u) = (v * v)$

preuve:

(1)	posons $w = (u * u)$	
(2)	posons $x = (v * v)$	
(3)	$(u * (u * u)) = u$	(théorème 3)
(4)	$(u * w) = u$	(3) (1) (ég.)
(5)	$(u * (v * v)) = u$	(théorème 3)
(6)	$(u * x) = u$	(5) (2) (ég.)
(7)	$(u * w) = (u * x)$	(4) (6) (ég.)
(8)	$w = x$	(7) (théorème 5)
(9)	$(u * u) = (v * v)$	(8)(1)(2) (ég.)

définition 1: Soit $y \in A$

$\alpha = (y * y)$

théorème 7: Soit $d, e, f \in A$

$d = ((e * ((e * f) * d)) * f)$

preuve:

(1)	posons $g = (e * f)$	
(2)	posons $h = (g * d)$	
(3)	posons $i = (e * h)$	
(4)	posons $j = (i * f)$	
(5)	posons $k = (g * j)$	
(6)	$i = (e * ((e * f) * (i * f)))$	(axiome)
(7)	$i = (e * (g * j))$	(6)(1)(4) (ég.)
(8)	$i = (e * k)$	(7) (5) (ég.)

(9)	$(e * h) = (e * k)$	(3) (8) (ég.)
(10)	$h = k$	(9) (théorème 5)
(11)	$(g * d) = (g * j)$	(10)(2)(5) (ég.)
(12)	$d = j$	(11)(théorème 5)
(13)	$d = (i * f)$	(12) (4) (ég.)
(14)	$d = ((e * h) * f)$	(13) (3) (ég.)
(15)	$d = ((e * (g * d)) * f)$	(14) (2) (ég.)
(16)	$d = ((e * ((e * f) * d)) * f)$	(15) (1) (ég.)

théorème 8: Soit $l, m \varepsilon A$

Il existe un et un seul n tel que $l = (n * m)$

preuve:

Il en existe un!

Il s'agit de prendre $n = (m * ((m * m) * l))$ puisque $l = ((m * ((m * m) * l)) * m)$ par le théorème 7, et ainsi $l = (n * m)$.

Il en existe au plus un!

Supposons qu'il y en a deux, disons n et o, ainsi $l = (n * m)$ et $l = (o * m)$, c'est-à-dire $(n * m) = (o * m)$ d'où $n = o$ par le théorème 5.

définition 2: Soit $p, q, r \varepsilon A$

$(p \# q) = r$ ssi $p = (r * q)$

théorème 9: Soit $s, t \varepsilon A$

$((s \# t) * t) = s$

preuve:

(1)	posons $u = (s \# t)$	
(2)	$s = (u * t)$	(1) (déf. 2)
(3)	$s = ((s \# t) * t)$	(2) (1) (ég.)

théorème 10: Soit $v, w \in A$

$(v \# w) = (w \# v)$

preuve:

(1)	posons $x = (v \# w)$	
(2)	$v = ((v \# w) \ast w$	(théorème 9)
(3)	$v = (x \ast w)$	(2) (1) (ég.)
(4)	$(x \ast v) = (x \ast (x \ast w))$	(3) (ég.)
(5)	$(x \ast (x \ast w)) = w$	(théorème 4)
(6)	$(x \ast v) = w$	(4) (5) (ég.)
(7)	$(w \# v) = x$	(6) (déf. 2)
(8)	$(w \# v) = (v \# w)$	(7) (1) (ég.)

théorème 11: Soit $d, e, f \in A$

$((d \# e) \# f = (d \# (e \# f))$

preuve:

(1)	posons $g = (d \# e)$	
(2)	posons $h = (g \# f)$	
(3)	posons $i = (e \# f)$	
(4)	$g = ((g \# f) \ast f)$	(théorème 9)
(5)	$g = (h \ast f)$	(4) (2) (ég.)
(6)	$e = ((e \# f) \ast f)$	(théorème 9)
(7)	$e = (i \ast f)$	(6) (3) (ég.)
(8)	$d = ((d \# e) \ast e)$	(théorème 9)
(9)	$d = (g \ast e)$	(8) (1) (ég.)
(10)	$d = ((h \ast f) \ast (i \ast f))$	(9)(5)(7) (ég.)
(11)	$(h \ast d) = (h \ast ((h \ast f) \ast (i \ast f)))$	(10) (ég.)
(12)	$(h \ast ((h \ast f) \ast (i \ast f))) = i$	(axiome)
(13)	$(h \ast d) = i$	(11) (12) (ég.)
(14)	$(i \# d) = h$	(13) (déf. 2)
(15)	$(i \# d) = (d \# i)$	(théorème 10)
(16)	$(d \# i) = h$	(14) (15) (ég.)
(17)	$(d \# (e \# f)) = (g \# f)$	(16)(3)(2) (ég.)
(18)	$(d \# (e \# f)) = ((d \# e) \# f)$	(17) (1) (ég.)

théorème 12: Soit $j \in A$

$(j \# \alpha) = j$ et $(\alpha \# j) = j$

preuve:

(1)	$(j * (j * j)) = j$	(théorème 3)
(2)	$(j * j) = \alpha$	(définition 1)
(3)	$(j * \alpha) = j$	(1) (2)
(4)	$(j \# \alpha) = j$	(3) (définition 2)
(5)	$(j \# \alpha) = (\alpha \# j)$	(théorème 10)
(6)	$(\alpha \# j) = j$	(4) (5)
(7)	$(j \# \alpha) = j$ et $(\alpha \# j) = j$	(4) (6)

théorème 13: Soit $k \in A$

Il existe $h \in A$ tel que $(k \# h) = \alpha$ et $(h \# k) = \alpha$

preuve:

Il s'agit de prendre $h = (\alpha * k)$

on peut déduire alors: $h \# k = \alpha$ par la définition 2.

Puis, avec la commutativité de # (théorème 10),

on a le résultat cherché.

théorème 14: $\langle A , \# , \alpha \rangle$ est un groupe abélien.

preuve:

Théorèmes 10- 11- 12- 13.