CGTM 53
September 1968

Dependence of Equality Axioms in Elementary Group Theory

George Robinson
Computation Group, Stanford Linear Accelerator Center

and

Lawrence Wos
Applied Mathematics Division, Argonne National Laboratory

September 1967

Revised October 1967

One approach to the treatment of equality in a formal axiomatic study of group theory is to accord to the equality symbol a special logical status by providing in the logical apparatus an inference rule allowing substitution of equal terms for one another. A slightly different approach is to axiomatize the equality predicate within ordinary first-order predicate calculus. Following the latter approach, one might give the following set of axioms for group theory.

A1	$(\exists z)\ xy=z$	closure
A2	$ex=x$	left identity
A3	$(\exists y)\ yx=e$	left inverse
A4	$xy=u,\ yz=v,\ uz=w \supset xv=w$	associativity (case 1)
A5	$xy=z,\ xy=u \supset z=u$	uniqueness of product
A6	$z=u,\ xy=z \supset xy=u$	substitution (3rd position)
A7	$z=u,\ xz=y \supset xu=y$	substitution (2nd position)
A8	$z=u,\ zx=y \supset ux=y$	substitution (1st position)
A9	$x=x$	reflexivity
A10	$x=y \supset y=x$	symmetry
A11	$x=y,\ y=z \supset x=z$	transitivity

The hybrid notation used above attempts to effect a compromise between the precision of conventional predicate calculus notation and the relative intuitive clarity of conventional mathematical notation. The implicit universal quantification on variables late in the alphabet, (except where explicit existential quantification is used), the use of a constant e, and the use of commas in place of the logical connective '$\wedge$' need only be noted in passing. The use of 'x=y' in place of, say, 'Rxy' and 'xy=z' in place of, say, 'Pxyz' will not lead to confusion so long as it is kept in mind (where necessary) that these are intended as two different predicates -- one binary and one ternary.

If we choose to think of A1-A4 in terms of a simple applied functional calculus with only the ternary predicate P (think of xy=z as Pxyz), and follow the method outlined by Church [1] for introducing an equality predicate R (think of x=y as Rxy), A6-A11 will be the axioms to be introduced. For the case of group theory, Abraham Robinson [2] gives essentially* the same formulation as A1-A11.

Given such a set of axioms, the question of dependence arises: Which, if any, of A1-A11 can be proved from the remaining ones? First it will be shown that A7-A11 can be derived from A1-A6.

It will be convenient to obtain two preliminary results:

T1: $xy=u,\ yz=v,\ xv=w \supset uz=w$ (associativity - case 2)

T2: $xe=x$ (right identity)

Taken together A4 and T1 can be written

$$xy=u,\ yz=v \supset (xv=w \equiv uz=w)$$

which is what one might be inclined to write for the associative law. Since (as will be seen from the following proof) T1 follows from A1-A6, A4 will suffice for associativity.

T1: ASSOCIATIVITY - (CASE 2)

1.	$xy=u,\ yz=v,\ uz=w \supset xv=w$	A4 (ASSOCIATIVITY -CASE 1)
2.	$xy=z,\ xy=u \supset z=u$	A5 (UNIQUENESS)
3.	$xv=w,\ xv=s \supset w=s$	$2\left(\begin{smallmatrix} y & z & u \\ v & w & s \end{smallmatrix}\right)$
4.	$xy=u,\ yz=v,\ uz=w,\ xv=s \supset w=s$	$1_4,\ 3_1$
5.	$z=u,\ xy=z \supset xy=u$	A6 (SUBSTITUTION - 3RD POSITION)
6.	$w=s,\ qt=w \supset qt=s$	$5\left(\begin{smallmatrix} z & u & x & y \\ w & s & q & t \end{smallmatrix}\right)$
7.	$xy=u,\ yz=v,\ uz=w,\ xv=s,\ qt=w \supset qt=s$	$4_5,\ 6_1$
8.	$xy=u,\ yz=v,\ uz=t,\ xv=w \supset uz=w$	$7\left(\begin{smallmatrix} q & t & w & s \\ u & z & t & w \end{smallmatrix}\right)$
9.	$(\exists t)\ uz=t$	A1 (CLOSURE)
10.	$xy=u,\ yz=v,\ xv=w \supset uz=w$	$9,\ 8_3$

---

* In place of A6-A8, he gives

$$s=t,\ v=w,\ x=y,\ sv=x \supset tw=y$$

which, in the presence of reflexivity, is equivalent to A6-A8.

T2: RIGHT IDENTITY:

1.	xy=u, yz=v, xv=w ⊃ uz=w	T1 (ASSOCIATIVITY - CASE 2)
2.	xe=u, ez=z, xz=w ⊃ uz=w	$1\binom{y\ v}{e\ z}$
3.	ez=z	A2 (LEFT IDENTITY)
4.	xe=u, xz=w ⊃ uz=w	$3, 2_2$
5.	xe=u ⊃ ue=u	$4\ \binom{z\ w}{e\ u}$
6.	xy=u, yz=v, uz=w ⊃ xv=w	A4 (ASSOCIATIVITY - CASE 1)
7.	xy=w, yz=e, wz=u ⊃ xe=u	$6\binom{w\ v\ u}{u\ e\ w}$
8.	xy=w, yz=e, wz=u ⊃ ue=u	$7_4, 5_1$
9.	xy=e, yz=e, ez=z ⊃ ze=z	$8\binom{w\ u}{e\ z}$
10.	xy=e, yz=e ⊃ ze=z	$3, 9_3$
11.	(∃x) xy=e	A3 (LEFT INVERSE)
12.	yz=e ⊃ ze=z	$11, 10_1$
13.	(∃y) yz=e	A3 (LEFT INVERSE)
14.	ze=z	$13, 12_1$

The proof of T2 (the usual one, but diluted somewhat by the poverty of A1-A6) is presented merely to show that the proof does not depend on A7-A11. (Similarly, the existence of right inverse could be deduced from A1-A6.)

Next we establish that A9 and A10 follow from A1-A6.

REFLEXIVITY:

1.	xy=z, xy=u ⊃ z=u	A5 (UNIQUENESS)
2.	ex=x, ex=u ⊃ x=u	$1\binom{x\ y\ z}{e\ x\ x}$
3.	ex=x	A2 (LEFT IDENTITY)
4.	ex=u ⊃ x=u	$3, 2_1$
5.	ex=x ⊃ x=x	$4\binom{u}{x}$
6.	x=x	$3, 5_1$

SYMMETRY:

1.	z=u, xy=z ⊃ xy=u	A6 (SUBSTITUTION - 3RD POS)
2.	xy=z, xy=u ⊃ z=u	A5 (UNIQUENESS)
3.	xy=u, xy=w ⊃ u=w	$2\binom{z\ u}{u\ w}$
4.	z=u, xy=z, xy=w ⊃ u=w	$1_3, 3_1$
5.	z=u, xy=z ⊃ u=z	$4\binom{w}{z}$

6.	$y=u,\ ey=y \supset u=y$	5 $\binom{z\ x}{y\ e}$
7.	$ey=y$	A2 (LEFT IDENTITY)
8.	$y=u \supset u=y$	7, 6_2

In a similar fashion A11 (transitivity) can be deduced from A2, A5 and A6. The remaining substitution axioms, A7 and A8 can be deduced from A4, A6, and T2 and A2, A6, and T1 respectively. The formal proofs are given in the appendix.

Thus, given A1-A6, one can deduce as theorems A7-A11 in ordinary first-order predicate calculus. What of A5 and A6? Viewed within the framework of ordinary first-order predicate calculus, are they further dependent on A1-A4? To answer this question, it is necessary to put aside any special equality properties of the predicate '=' we may have found intuitively helpful in following the proofs given earlier. For the moment, $x=y$ is to be thought of merely as an arbitrary binary predicate Rxy which may or may not have the familiar equality properties (e.g., it may fail to be reflexive). Now consider the set of ordered triples $P = \{(e,e,e), (e,a,a), (a,e,a), (a,a,e)\}$ (a familiar group operation on two elements), and first let $R = \emptyset$. Then, of A1-A6, all are satisfied but A5 since $z \neq u$, and hence A6, is true for all choices of x, y, z, and u, but $ee=e,\ ee=e \supset e=e$ is false (because $e=e$ is false in this model, since $(e,e) \notin R$). Thus uniqueness of product is independent of the remaining axioms. Similarly 3rd position substitution is independent; for consider P as before but let R be the set $\{e,a\} \times \{e,a\}$. Then $z=u$, and hence uniqueness, is true for all choices of x, y, z, and u, but $e=a,\ ee=e \supset ee=a$ is false.

The axioms A6-A8 can be written in the form

$$\text{C1:}\quad (z)(u)\{(z=u) \supset (x)(y)\,[(xy=z \equiv xy=u) \wedge (xz=y \equiv xu=y) \wedge (zx=y \equiv ux=y)]\}.$$

The consequent of the conditional in C1 can be thought of as a necessary condition for the equality of elements z and u. Quine [3] gives a slightly different and rather interesting approach. He makes the necessary condition of C1 <u>sufficient</u> as well:

$$\text{C2:}\quad (z)(u)\ \{(x)(y)[(xy=z \equiv xy=u) \wedge (xz=y \equiv xu=y) \wedge (zx=y \equiv ux=y)] \supset (z=u)\}.$$

By showing that A9-A11 follow from C1 and C2, he dispenses with the equivalence relation axioms. That C1-C2 is <u>strictly</u> stronger than, say C1 and A9-A11 may be seen by taking $P = \{e,a\} \times \{e,a\} \times \{e,a\}$ and $R = \{(e,e), (a,a)\}$. Nevertheless C2 is still derivable from A1-A6. To show this, we first derive from A1-A6

$$C3: (z)(u) \{(x)(y) [xy=z \equiv xy=u] \supset z=u\} \quad .$$

The negation of C3 can be written as the conjunction of three clauses:

1. $a \neq b$
2. $xy=a \supset xy=b$
3. $xy \neq a \supset xy \neq b$.

The refutation proceeds as follows:

4.	$xy=z,\ xy=u \supset z=u$	A5 (uniqueness)
5.	$xy=a,\ xy=b \supset a=b$	$4\binom{z\ u}{a\ b}$
6.	$xy=a \supset a=b$	$2_2,\ 5_2$
7.	$xy \neq a$	$1,\ 6_2$
8.	$ea \neq a$	$7\binom{x\ y}{e\ a}$

but 8 is inconsistent with A2.

Thus the negation of C3 is inconsistent with A1-A6 and hence C3 must be a theorem of A1-A6. By inspection C2 is seen to be a consequence of C3 and hence a theorem of A1-A6.

Conclusion:

Although, for an arbitrary ternary predicate Pxyz, six axioms (A6-A11) are needed to introduce and relate the equality predicate Rxy to Pxyz; if Pxyz has the properties of a group operation (A1-A5) only A6 is needed. Another way to look at this is that if an arbitrary binary predicate Rxy is related to a group operation in the manner required by A5 and A6, it cannot be distinguished (insofar as the group operation is concerned) from the usual equality relation.

References

1. Church, A. Introduction to Mathematical Logic, Vol. I, Princeton Univ. Press, Princeton, N.J., 1956, p. 283 (ex. 48.4).

2. Robinson, Abraham. Introduction to Model Theory and to the Metamathematics of Algebra, North Holland Publishing Co., Amsterdam, 1963, pp 23-26.

3. Quine, W.V.O. Set Theory and Its Logic, Belknap Press Harvard, Cambridge, Massachusetts, 1963, pp. 12-15.

APPENDIX: Proofs of A7, A8, and A11

TRANSITIVITY:

1.	$z=u,\ xy=z \supset xy=u$	A6(SUBSTITUTION-3RD POS)
2.	$y=u,\ ey=y \supset ey=u$	$1\begin{pmatrix} z & x \\ y & e \end{pmatrix}$
3.	$ey=y$	A2(LEFT IDENTITY)
4.	$y=u \supset ey=u$	$3,\ 2_2$
5.	$u=w,\ ey=u \supset ey=w$	$1\begin{pmatrix} u & x & z \\ w & e & u \end{pmatrix}$
6.	$y=u,\ u=w \supset ey=w$	$4_2,\ 5_2$
7.	$xy=z,\ xy=u \supset z=u$	A5 (UNIQUENESS)
8.	$ey=t,\ ey=w \supset t=w$	$7\begin{pmatrix} x & z & u \\ e & t & w \end{pmatrix}$
9.	$y=u,\ u=w,\ ey=t \supset t=w$	$8_2,\ 6_3$
10.	$y=u,\ u=w,\ ey=y \supset y=w$	$9\begin{pmatrix} t \\ y \end{pmatrix}$
11.	$y=u,\ u=w \supset y=w$	$3,\ 10_3$

SUBSTITUTION-FIRST POSITION

1.	$z=u,\ xy=z \supset xy=u$	A6 (SUBST-3RD POS)
2.	$y=u,\ ey=y \supset ey=u$	$1\begin{pmatrix} z & x \\ y & e \end{pmatrix}$
3.	$ey=y$	A2 (LEFT IDENTITY)
4.	$y=u \supset ey=u$	$3,\ 2_2$
5.	$xy=u,\ yz=v,\ xv=w \supset uz=w$	T1 (ASSOCIATIVITY - CASE 2)
6.	$ey=u,\ yz=v,\ ev=w \supset uz=w$	$5\begin{pmatrix} x \\ e \end{pmatrix}$
7.	$y=u,\ yz=v,\ ev=w \supset uz=w$	$6_1,\ 4_2$
8.	$x=u,\ xz=y,\ ey=y \supset uz=y$	$7\begin{pmatrix} y & v & w \\ x & y & y \end{pmatrix}$
9.	$x=u,\ xz=y \supset uz=y$	$3,\ 8_3$

SUBSTITUTION- SECOND POSITION

1.	$z=u,\ xy=z \supset xy=u$	A6 (SUBST-3RD POS)
2.	$x=u,\ xe=x \supset xe=u$	$1\begin{pmatrix} z & y \\ x & e \end{pmatrix}$
3.	$xe=x$	T2 (RIGHT IDENTITY)
4.	$x=u \supset xe=u$	$3,\ 2_2$
5.	$xy=u,\ yz=v,\ uz=s \supset xv=w$	A4 (ASSOCIATIVITY -CASE 1)
6.	$yx=z,\ xe=u,\ ze=w \supset yu=w$	$5\begin{pmatrix} y & z & v & x & u \\ x & e & u & y & z \end{pmatrix}$
7.	$x=u,\ yx=z,\ ze=w \supset yu=w$	$6_2,\ 4_2$
8.	$z=u,\ yz=x,\ xe=x \supset yu=x$	$7\begin{pmatrix} z & w & x \\ x & x & z \end{pmatrix}$
9.	$z=u,\ yz=x \supset yu=x$	$3,\ 8_2$