Mathematical Theories

Robert Keller
7 February 2005

Theories

- In logic, a **Theory** is a set of formulas called **theorems**. The formulas are derived from a basis set of **axioms** using the inference rules.

- To avoid enumerating all the axioms each time, we will use the notation:

  $$\Gamma \vdash \psi$$

  where Γ is a **set** of formulas, to mean that ψ can be derived from formulas in Γ.

- Note that Γ could be **infinite**, even though in a given proof, however, only a finite set of the axioms could actually be used. (Over *all* proofs, an unbounded set of axioms could be used.)

Group Theory as an Example

- We'll use group theory as an illustrative example.
- Since this is a course on logic rather than algebra, take this theory as indicative of a very small slice of the picture.
- Group theory has many applications:
  - Coding theory (error-correcting codes)
  - Computer architecture (processor-memory interconnect)
  - Quantum physics (particle spins)
  - Chemistry
  - Interior decorating

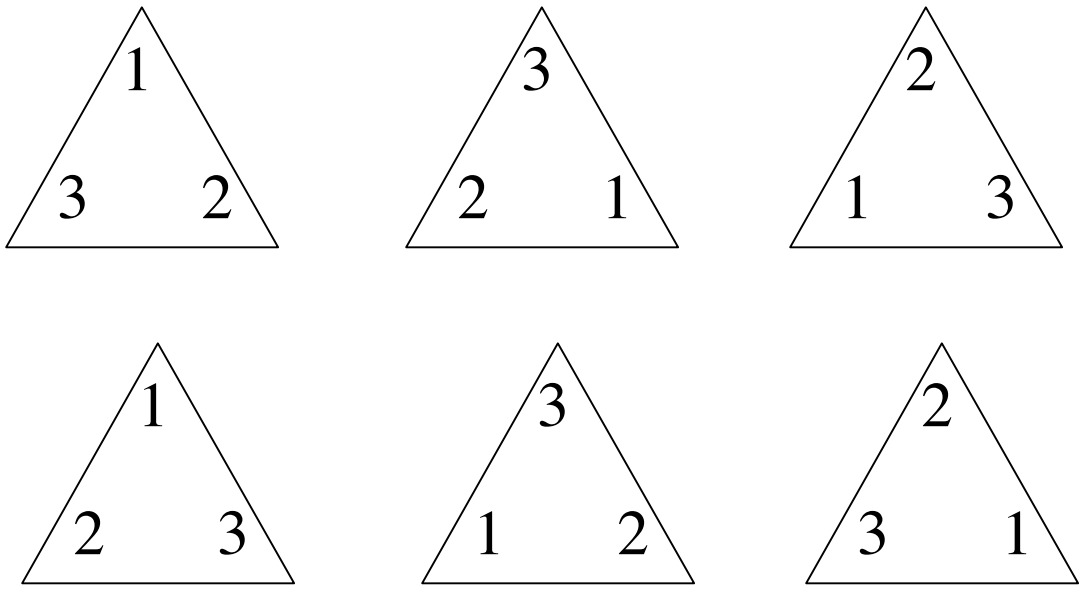
A Really Simple Example

- Dihedral groups express the symmetries of a planar figure that can be rotated or reflected (or flipped over).

- There are dihedral groups D_n of 2n elements for each natural number n.

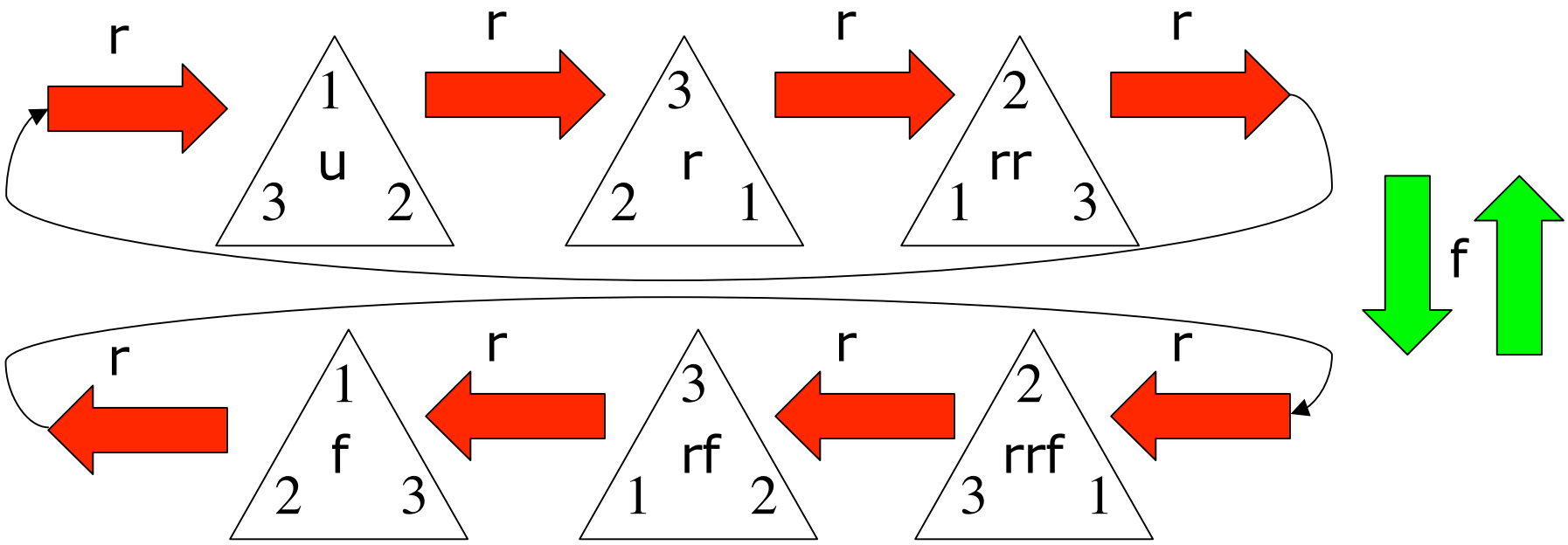
Example: Dihedral Group D_3

- Consider the symmetries of an equilateral triangle with identifiable vertices



Example: Dihedral Group D_3

- Identify the first position as the unit (arbitrarily) u
- Identify each position with **a** sequence of rotations (r) and flips (f) that can be used to take the unit to that position [The designation won't be unique; pick one.]



Example: Dihedral Group D_3

- Create a composition table for doing one transformation after the other

	u	r	rr	f	rf	rrf
u						
r						
rr						
f						
rf						
rrf						

Example: Dihedral Group D_3

- The table thus created defines our group operation.
- Verify the group properties:
  - Associativity
  - Identity
  - Inverse
- Inverse table

x	u	r	rr	f	rf	rrf
i(x)						

Other Dihedral Groups

(from http://server1.fandm.edu/departments/Mathematics/a.crannell/hm/Math/dihedral.html)

Dihedral Group	Symbol	Our Thoughts
D_1		Shell gas uses the symbol to the left. This shell shape has no rotations (other than the identity) and has only one mirror line (vertical). Therefore, like Mickey Mouse, the figure is said to be bilaterally symmetric and it fits into the category D_1.
D_2		An example of D_2 that is easily spotted is the logo for the Central Broadcasting System (CBS). The "eye" shape within the circle prevents the figure from being able to rotate by any rotation other than a 1/2 turn. Additionally, the figure has only two ways in which it can be reflected onto itself.
D_3		The luxury car, Mercedes-Benz, uses a symbol with three rotations and 3 mirror lines. Therefore, the emblem is an example of D_3. If we were to convert this figure into a peace sign, however, we would lose 2 of the rotations and two of the reflection lines. This would leave a D_1 figure.
D_4		The symbol for Purina is a great example of a finite figure of the category D_4. It is easy to see that there are four mirror reflections of the figure (one vertical, one horizontal, and two diagonal) as well as four rotations. In other words, rotating the figure four times gives the original figure (the identity).
D_5		The symbol for Chrylser is a great example of a finite figure of the category D_5. In other words, the symbol has five rotations and five axes of reflection.
D_8		This finite figure is a dihedral group of order 8 due to its eight reflections and eight rotations. The symmetries are created by two squares placed on top of each other and offset by 90 degrees.

Example: Group Theory, one formulation

- There are two function symbols:
  - f which is 2-ary, the **group operator**
  - i which is 1-ary, the **inverse** function
- There is one constant symbol u, the unit or identity.
- = is the only predicate symbol.

- G1: $(\forall x)(\forall y)(\forall z)\ f(x, f(y, z)) = f(f(x, y), z)$ [associative law]

- G2R:$(\forall x)\ f(x, u) = x$ ["R" stands for "right".]

- G3R:$(\forall x)\ f(x, i(x)) = u$ [i(x) is the inverse of x.]

- A pair of alternates for G2R, G3R is:
  G2R':$(\forall x)\ (f(x, u) = x \wedge f(u, x) = u))$
  G3R':$(\forall x)(\exists y)\ (f(x, y) = u \wedge f(y, x) = u)$
- i can be thought of as a "Skolem function"

Group Theory Proof Example 1

- G3L:(∀x) f(i(x), x) = u
- Before attempting to construct a formal proof, it is wise to have an **informal plan**.
- Our plan is based on experimenting with some trial equalities and more convenient notation:

- We write (x y) for f(x, y) and x’ for i(x).

- Restating the axioms with this notation:
- G1: (∀x)(∀y)(∀z) (x (y z)) = ((x y) z)
- G2R:(∀x) (x u) = x
- G3R:(∀x) (x x’) = u

- We are also going to use the equality rules and derived rules in a somewhat cavalier fashion, to keep things simple.

Group Theory Proof Plan (Ex 1)

- G1: (∀x)(∀y)(∀z) (x (y z)) = ((x y) z)
- G2R:(∀x) (x u) = x
- G3R:(∀x) (x x′) = u
- Derive G3L:(∀x) (x′ x) = u

1.	((x′ x) u) = (x′ x)	by ∀e from G2R with (x′ x) replacing x
2.	(x′ (x′)′) = u	by ∀e from G3R with x′ replacing x
3.	((x′ x) (x′ (x′)′)) = (x′ x)	substituting (x′ (x′)′) for u in 1.
4.	(x′ ((x x′) (x′)′)) = (x′ x)	by ∀e from G1 on the l.h.s. of 3
5.	(x x′) = u	by ∀e from G3R
6.	(x′ (u (x′)′)) = (x′ x)	substituting u for (x x′) in 4
7.	((x′ u) (x′)′) = (x′ x)	by ∀e from G1 on the l.h.s. of 6
8.	(x′ (x′)′) = (x′ x)	by ∀e from G2R with x′ replacing x
9.	u = (x′ x)	from 8 and 2, using equality
10.	(x′ x) = u	from 9 and symmetry of equality

Group Theory Proof in More Detail (Ex 1)

(Underlines show items substituted for others later.)

- Proof of: G3L:(∀x) f(i(x), x) = u

1.	(∀x)(∀y)(∀z) f(x, f(y, z)) = f(f(x, y), z)	G1
2.	(∀x) f(x, u) = x	G2R
3.	(∀x) f(x, i(x)) = u	G3R
4.	x	
5.	f(f(i(x), x), u) = f(i(x), x)	∀e 2 [f(i(x), x) replaces x]
6.	f(i(x), i(i(x))) = u	∀e 3 [i(x) replaces x]
7.	f(f(i(x), x), f(i(x), i(i(x))) = f(i(x), x)	= subst. of l.h.s. of 6 for u in 5
8.	f(i(x), f(f(x, i(x)), i(i(x))) = f(f(i(x), x), f(i(x), i(i(x)))	∀e 1 (3 steps)
9.	f(i(x), f(f(x, i(x)), i(i(x))) = f(i(x), x)	= subst. 7, 8
10.	f(x, i(x)) = u	∀e 3 [x replaces x]
11.	f(i(x), f(u, i(i(x))) = f(i(x), x)	= subst. of u for f(x, i(x)) in 9
12.	f(i(x), f(u, i(i(x))) = f(f(i(x), u), i(i(x)))	∀e 1 (3 steps)
13.	f(f(i(x), u), i(i(x))) = f(i(x), x)	= subst. 11, 12
14.	f(i(x), u) = i(x)	∀e 2 [i(x) replaces x]
15.	f(i(x), i(i(x))) = f(i(x), x)	= subst. 13, 14
16.	u = f(i(x), x)	= subst. 15, 6
17.	f(i(x), x) = u	symmetry of = 16
18.	(∀x) f(i(x), x) = u	∀i 4-17

Group Theory Proof Example 2

- Derive G2L:(∀x) f(u, x) = x
- (We can use G3L, which was just proved.)

1.	(∀x)(∀y)(∀z) f(x, f(y, z)) = f(f(x, y), z)	G1
2.	(∀x) f(x, u) = x	G2R
3.	(∀x) f(x, i(x)) = u	G3R
4.	(∀x) f(i(x), x) = u	G3L
5.	x	
6.	f(u, x) = f(u, x)	=i
7.	f(x, i(x)) = u	∀e 3 [replace x with x]
8.	f(f(x, i(x)), x) = f(u, x)	= subst. 7 for u in 6
9.	f(x, f(i(x), x)) = f(f(x, i(x)), x)	∀e 1 (3 steps)
10.	f(x, f(i(x), x)) = f(u, x)	= subst. 9 in 8
11.	f(i(x), x) = u	∀e 4 [replace x with x]
12.	f(x, u) = f(u, x)	= subst. u 11 in 10
13.	f(x, u) = x	∀e 2 [replace x with x]
14.	x = f(u, x)	= subst. 13 in 12
15.	f(u, x) = x	symmetry of = 14
16.	(∀x) f(u, x) = x	

Group Theory Proof Example 3

- $(\forall x)(\forall y)(\forall z)\ f(x, y) = f(x, z) \rightarrow y = z$ G4R

- **Idea/Plan**
- Assume $f(x, y) = f(x, z)$
- $i(x) = i(x)$ =i
- Then $f(i(x), f(x, y)) = f(i(x), f(x, z))$ by = subst.
- Then $f(f(i(x), x), y) = f(f(i(x), x), z)$ by G1 (twice)
- Then $f(u, y) = f(u, z)$ by G3L (twice)
- Then $y = z$ by G2L (twice)

Group Theory Proof Example 4

- $(\forall x)(\forall y)(\forall z)\ f(x, z) = f(y, z) \rightarrow x = y$ G4L

- **Idea/Plan**
- Assume $f(x, z) = f(y, z)$
- $i(z) = i(z)$ =i
- Then $f(f(x, z), i(z)) = f(f(y, z), i(z))$ by = subst.
- Then $f(x, f(z, i(z)) = f(y, f(z, i(z))$ by G1 (twice)
- $f(z, i(z)) = u$ by G3R
- Then $f(x, u) = f(y, u)$ by = subst
- Then $x = y$ by G2R (twice)

Group Theory Exercises

- Derive from the axioms and theorems derived thus far:
- $(\forall x)\ (i(i(x)) = x)$
- $(\forall x)\ (\forall y)\ (i(f(x, y)) = f(i(y), i(x)))$
- $(\forall x)(\forall y)\ ((f(x, y) = e) \rightarrow (y = i(x)))$
- $(\forall x)(\forall y)\ ((f(x, y) = e) \rightarrow (x = i(y)))$
- $((\forall x)\ (f(x, x) = e)) \rightarrow ((\forall x)(\forall y)\ (f(x, y) = f(y, x)))$

Abelian Groups

- These are groups in which the group operator is commutative:

$$(\forall x)(\forall y)\ (f(x, y) = f(y, x))$$