

MA2C03 - DISCRETE MATHEMATICS - TUTORIAL NOTES

Brian Tyrrell

1 & 2/11/2016

1 Formal deduction

Example 1.1. Suppose we are told the following;

If turtles can sing then artichokes can fly. Artichokes can fly implies turtles can sing and dogs can't play chess. Dogs can play chess if and only if turtles can sing. Deduce that turtles can't fly.

Proof.

We convert these statements into a logical format;

P = "turtles can sing".

Q = "artichokes can fly".

R = "dogs can't play chess".

We can assume the following hypotheses from the above paragraph;

(a) $P \rightarrow Q$

(b) $Q \rightarrow (P \wedge R)$

(c) $\neg R \leftrightarrow P$

We wish to prove $\neg P$. We do so as follows:

(1) $Q \rightarrow (\neg R \wedge R)$ - substitution of (c) into (b).

(2) $\neg(\neg R \wedge R) \rightarrow \neg Q$ - contrapositive of (1).

(3) $\neg(\neg R \wedge R)$ - tautology.

(4) $\neg Q$ - MP (2, 3).

(5) $\neg Q \rightarrow \neg P$ - contrapositive of (a).

(6) $\neg P$ - MP (4, 5)

■

I was asked two questions regarding this - why can't we take a conjunction of our hypotheses and determine $\neg P$ from a truth table, and why can't we use a tautology involving the conjunction of all the hypotheses.

To answer this, first let's consider a simpler example;

Example 1.2. From $\neg Q$, $P \rightarrow Q$ deduce $\neg P$.

Proof.

Using formal deduction, this is proven by using the contrapositive of $P \rightarrow Q$, then modus ponens.

If we drew a truth table for these hypotheses;

P	Q	$\neg Q$	$P \rightarrow Q$	$\neg Q \wedge (P \rightarrow Q)$	$\neg P$
T	T	F	T	F	F
T	F	T	F	F	F
F	T	F	T	F	T
F	F	T	T	T	T

We see $\neg Q \wedge (P \rightarrow Q)$ and $\neg P$ disagree, thus are not equivalent. However $(\neg Q \wedge (P \rightarrow Q)) \rightarrow \neg P$ is a tautology (which, however, if you wanted to use you would need to prove using a truth table mid question). For argument's sake let us try use this tautology in formal deduction:

Hypotheses

(a) $\neg Q$

(b) $P \rightarrow Q$

We wish to prove $\neg P$. We attempt as follows;

(1) $\neg Q$ - (a).

(2) $\neg Q \rightarrow \neg P$ - contrapositive of (b).

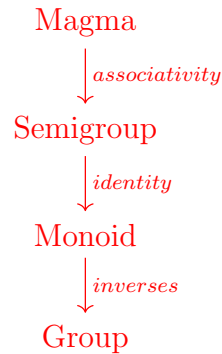
(3) $(\neg Q \wedge (P \rightarrow Q)) \rightarrow \neg P$ - tautology.

However we become stuck at (3) - we wish to use modus ponens to obtain $\neg P$, however to do so we need $\neg Q \wedge (P \rightarrow Q)$ **which we don't have**. We have $\neg Q$ and $P \rightarrow Q$ but we can't deduce $\neg Q \wedge (P \rightarrow Q)$ (without delving deeper into proof theory and logic and working through other theorems and lemmas).

In short, formal deduction (as presented in *Example 1.1*) is the only way we can tackle these types of questions in general, and this method will be the easiest, fastest and only correct approach we will cover. ■

2 Abstract algebra

To give some motivation for defining structures like *semigroup*, *monoid* and *group* we looked at the following diagram;



where:

Definition 2.1. A *magma* is a set Q with a binary operation $*$. The binary operation is *closed* (i.e. $\forall x, y \in Q, x * y \in Q$).

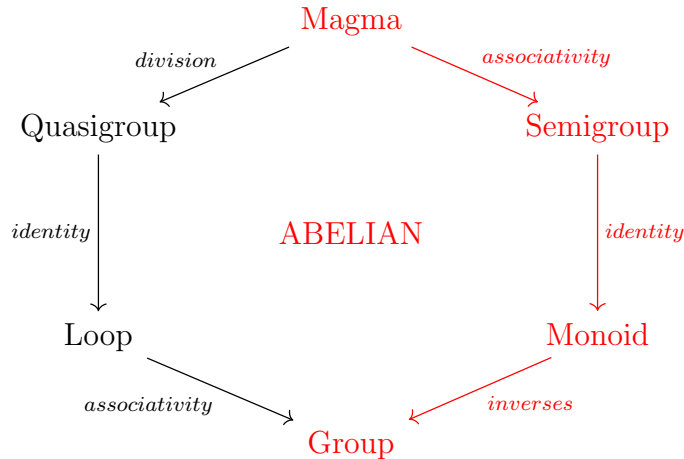
Definition 2.2. A magma where the binary operation is associative is known as a *semigroup*.

Definition 2.3. A semigroup with an identity element is called a *monoid*.

Definition 2.4. A monoid where every element has an inverse is known as a *group*.

Definition 2.5. A structure is called *abelian* if the operation is commutative.

As an aside, we can build from a magma to a group in a different way;



A magma where division is possible is called a *quasigroup*. If a quasigroup has an identity element, it's known as a *loop*. If the binary operation in the loop is associative, we have a group. The side you'll need to know for homework and exams is in **red**.

Example 2.1. Let A be a set. Prove $(P(A), \cup, \emptyset)$ is an abelian monoid.

Proof.

In order to prove a set with an operation is a magma, semigroup, monoid, etc, we just prove the set and operation obey the definition of the structure we're trying to prove it is.

In particular, here we're going to show \cup is associative, commutative and \emptyset is an identity element.

- (1) *Associativity.* We wish to show $\forall X, Y, Z \in P(A), X \cup (Y \cup Z) = (X \cup Y) \cup Z$. As we spoke about in tutorial 1, we do this by proving $X \cup (Y \cup Z) \subseteq (X \cup Y) \cup Z$ and vice versa:

Let $x \in X \cup (Y \cup Z)$. Then $x \in X$ OR $x \in Y \cup Z$ meaning $x \in X$ OR $x \in Y$ OR $x \in Z$ thus $x \in (X \cup Y) \cup Z$ as required. The reverse inclusion proof is the same.

(2) *Commutativity*. We wish to show $X \cup Y = Y \cup X$.

Again,

$$x \in X \cup Y \Rightarrow x \in X \text{ OR } x \in Y \Rightarrow x \in Y \text{ OR } x \in X \Rightarrow x \in Y \cup X$$

so $X \cup Y \subseteq Y \cup X$ and the reverse inclusion is the same argument. We can replace the " \Rightarrow " by " \Leftrightarrow " here.

(3) *Identity*. We wish to show $X \cup \emptyset = \emptyset \cup X = X$. We do this as follows;

Let $x \in X \cup \emptyset$. Then $x \in X$ OR $x \in \emptyset$. By definition of \emptyset we conclude $x \in X$.

Therefore $X \cup \emptyset \subseteq X$, and we know by definition of \cup , $X \subseteq X \cup \emptyset$. Thus $X \cup \emptyset = X$, and by the same proof we get $\emptyset \cup X = X = X \cup \emptyset$ as required.

Therefore $(P(A), \cup, \emptyset)$ is a monoid, as required. ■

Magmas, semigroups and monoids are quite simple structures, meaning examples are easily thought of - $(\mathbb{Z}, +, 0)$, $(\mathbb{R}, \times, 1)$, $(M_{n \times n}, *, I_n)$ are all monoids, the last one being an example of a *nonabelian* monoid. But not everything is one of these structures; $(\mathbb{Q}, \times, 1)$ *isn't* a group (as 0 has no inverse) but $(\mathbb{Q} \setminus \{0\}, \times, 1)$ is. We'll speak more about groups next week.

Remark. Veitch diagrams will not be accepted as a form of proof in set theory.