2F : Foundations of Pure Mathematics

Ken Brown

Joao Almeida-Domingues[*]

University of Glasgow

September 23rd, 2019 – December 5th, 2019

Contents

These lecture notes were collated by me from a mixture of sources , the two main sources being the lecture notes provided by the lecturer and the content presented in-lecture. All other referenced material (if used) can be found in the *Bibliography* and *References* sections.

The primary goal of these notes is to function as a succinct but comprehensive revision aid, hence if you came by them via a search engine , please note that they're not intended to be a reflection of the quality of the materials referenced or the content lectured.

Lastly, with regards to formatting, the pdf doc was typeset in LaTeX, using a modified version of Stefano Maggiolo's class

[*]2334590D@student.gla.ac.uk

1 Sets

1.1 definition. Set : an unordered collection of objects, which we call its *elements/members*

1.2 notation. $A = \{a, b, c\}$, represents a set A with members a, b, c

1.3 notation. It is conventional to use capital letters to denote sets, and lowercase ones for their members

1.4 notation. $x \in A$, means that the element x belongs to the set A

Instead of listing a members of a set exhaustively, we can define a rule whose truth value tells us if a given object should be a member of the set

1.5 notation. $A = \{x | P(x)\}$,where $P(x)$ can be any statement with a truth value (e.g. *"has 2 legs"* , $x > 0$)

1.6 definition. Subset : a set whose elements belong to another set of equal or larger size.

$$A \subset B = \{x \mid \forall\ x \in A\ ,\ x \in B\}$$

1.7 remark. Subsets can be differentiated into *proper* , if $A \neq B$, or *improper* if $A = B$.

1.8 notation. $A \subset B$, reads as *"A is a subet of B"*. $\subseteq$ for improper

1.9 notation. $\emptyset$ is the empty set, the set who has no members

1.10 remark. $\emptyset \subset S \forall S$

☛ **1.11 definition. Equality** $A = B \iff A \subseteq B$ and $B \subseteq A$

1.12 definition. Power Set is the set composed by all possible combinations of a sets members

1.13 notation. $P(X)$ or 2^X

1.14 example. Let $X = \{1, 2, 3\}$, then $P(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$

TODO **1.15 theorem.** *For* $|S| = n$, $|P(S)| = 2^n$

Proof. QED

1.16 definition. Union set of all elements belonging to *at least one* of the sets

$$A \cup B = \{x | x \in A \text{ or } x \in B\}$$

1.17 notation. $A \cup B$

1.18 definition. Intersection set of all elements which are part of both sets

$$A \cap B = \{x | x \in A \text{ and } x \in B\}$$

1.19 notation. $A \cap B$

1.20 theorem. *The union of sets is associative, i.e* $(A \cup B) \cup C = A \cup (B \cup C)$

Proof.

Our **first step** , is to understand what it is that the sentence actually says. We have an equality , by the definition of equality *(1.11)*, we need to show that **(1)** LHS $\subseteq$ RHS , and **(2)** the converse.

At this stage we have two tasks to accomplish, which seem to have something in common. Note that both require showing that one set is a subset of another. So, our **second step** should be to figure out, what being a subset means, again resorting to a definition. So, by *(1.6)* we have that for an arbitrary x chosen from the subset , x must also be in its parent set.

Hence, starting with **(1)**, our next step is to show that for an arbitrary x in $(A \cup B) \cup C = A$, x is also in $A \cup (B \cup C)$. Therefore, we assume that $x \in (A \cup B) \cup C = A$. What does that mean? It means that $x \in A \cup B$ or $x \in C$. Hence, $x \in A$ or $x \in B$ or $x \in C$.

Now, we have deconstructed, as it were, our compound statement into simpler ones. At this stage it's usually good to look back at what we are trying to prove. It seems very similar to what we have. We seem to have "atomic" building blocks, and we need only to start building it again into a compound statement.

Note that $x \in B$ or $x \in C$, just means $x \in B \cup C$. Finally, from $x \in A$ or $x \in B \cup C$ we get $A \cup (B \cup C) =$ RHS , as required

(2) will be omitted, as (1) is painstakingly detailed, and should work as a template

QED

1.21 remark. It is key in this type of set proofs to assume that some arbitrary element is in a set and show that it is (or is not) in the other. The rest is common to many other proofs where one aims to "unpack" the definitions enough until reaching a point where the expression matches the other side of the equality, or it can be built upon so as to match it

Both the union and the intersection are associative. Formally, we write:

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n$$

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n$$

2 Functions

3 Relations

4 Modular Arithmetic

4.1 definition. Congruence For $a, b, m, k \in \mathbb{Z}, a \equiv b \mod m \iff (a-b)k = m$. We say that *"a is congruent to b modulo m"*. a, b share the same remainder when divided by m

4.2 definition. Congruence Classes For $m \in \mathbb{Z}$, each congruence class represents a partition of $\mathbb{Z}$. Each partition represents all possible remainders $\{0, \ldots, m-1\}$ when diving the elements within it by m

4.3 example. Take , $m = 3$

$$[0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$
$$[1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$$
$$[2] = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$$

4.4 remark. Note that each partition is unique, but we can replace the number inside the brackets by any member of the class. $[0] = [3] = [60]$, since $0 \mod 3 = 3 \mod 3 = 60 \mod 3 = 0$

4.5 theorem. *If $a \equiv b \mod m$ and $c \equiv d \mod m$, then*

$$a \pm c \equiv b \pm d \mod m \qquad \text{and} \qquad ac = bd \mod m$$

4.6 lemma. *It follows from the above theorem that operating on classes, is the same as operating on their representatives (since each rep is a placeholder for the same remainder)*

$$[a] + [c] := [a + c]$$
$$[a] - [c] := [a - c]$$
$$[a][c] := [a]$$

4.7 example. Show that $n^2 \equiv 1 \mod 8$ for every odd integer n . If n is odd, then it must be congruent to an odd representative, i.e it must belong to one of the following possible classes $[1], [3], [5], [7]$. $n^2 = n \times n$. Hence, n^2 must belong to $[1 \times 1], [3 \times 3], [5 \times 5], [7 \times 7] = [1], [9], [25], [49] = [1]$. Therefore $n^2 = 1 \mod 8$

4.1 *Linear Congruences*