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

QED

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

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 , $m = 3$

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

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*

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

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)*

$$\begin{aligned} &[a] + [c] := [a + c] \\ &[a] - [c] := [a - c] \\ &[a][c] := [a] \end{aligned}$$

4.7 example. Show that $n^2 \equiv 1 \bmod 8$ 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

5 Permutations

5.1 definition. Permutation A permutation of X is a bijective function from X to X

5.2 notation. $\text{Perm}(X)$, set of permutations of X

5.3 definition. **Group** A group G is a finite or infinite set of elements together with a binary operation , *the group operation*, that together satisfy the four fundamental properties of closure, associativity, the identity property, and the inverse property.

5.4 definition. **Symmetric Group** of degree n is the group of all permutations on n symbols

5.5 notation. S_n

5.6 theorem. $\|S_n\| = n!$

Permutations can be represented in one of three ways

5.7 notation. Two-Line

$$\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$$

where $a_1, \dots, a_n$ is a list of the members of X and where $\sigma(a_i) = b_i$

5.8 notation. One-Line

$$b_1\, b_2 \dots b_n$$

5.9 notation. Permutation cycles

$$(a_1 b_2 a_3 b_1)(b_3 a_2)$$

5.10 remark. Generally, elements of X which map onto themselves , i.e $a_i \mapsto a_i = (a_i)$, are not explicitly represented

5.11 definition. **Cycle** a permutation of the elements of X which maps the elements of a subset $S = a_1, ..., a_k \mapsto X$ to each other in a cyclic fashion

5.12 definition. **Transposition** k-cycle, with $k = 2$

So, for example, the bijection rules for the two cycles introduced above, are respectively :

$$a_1 \mapsto b_2 \mapsto a_3 \mapsto b_1 \mapsto a_1 \text{ and } b_3 \mapsto a_2 \mapsto b_3$$

5.13 definition. **Disjoint Cycles** two cycles A, B are disjoint if $\forall\, a, b \in A, B\ a \neq b$

5.14 lemma. *disjoint cycles commute*

This should be clear, from the fact that each disjoint set only maps onto itself

Computation Constructing Cycles

1. Apply the mapping for each $\sigma(a_k)$
2. If $\sigma(a_k) = a_k$, close the cycle
3. Repeat (1) , (2) untill all elements in X have been mapped

5.15 remark. In particular , most texts have the operation being right-associative, i.e for $(xy)(zy)$ one has $z \mapsto y \mapsto x$ and not $x \mapsto y \mapsto z$

5.16 example. Express $\sigma, \tau, \sigma\tau, \tau\sigma$ and σ^{-1} as compositions of disjoint cycles.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$$

We consider what happens to each element of $\{1, \ldots, 5\}$ when σ is applied repeatedly. The action of σ can be described as

$$1 \mapsto 2 \mapsto 5 \mapsto 1, \quad 3 \mapsto 4 \mapsto 3,$$

so $\sigma = (1,2,5)(3,4)$. Similarly

$$\tau = (1,3)(2,5,4), \sigma\tau = (1,4,5,3,2)$$
$$\tau\sigma = (1,5,3,2,4), \sigma^{-1} = (1,5,2)(3,4)$$

Note that this is a composition , which in general is not commutative for non-disjoint cycles. In particular, we can think of each cycle having its own function σ, θ, etc , where mapping elements between cycles corresponds to their composition $\theta(\sigma(a_k)) = a_k \mapsto \sigma(a_k) \mapsto \theta(\sigma(a_k))$. Hence, the order is important

Computation Product of Cycles

1. Map each element between cycles, starting from the right
    (a) Pick an element from right cycle, map to the left until either the leftmost cycle is reached (or it is not present in any "to-the-left" cycles [see remark])
2. Repeat (1) , taking the last mapped as the starting element
3. Repeat until all elements are in a cycle

5.17 example.

$$\tau = (1,2,6)(2,4,6)(3,7)(2,6)$$

$\mathbf{2} \mapsto 6 \mapsto 2 \mapsto 6 \quad (2\ 6\ \ldots)$ All cycles covered

$6 \mapsto 2 \mapsto 4$ $(2\ 6\ 4\ \ldots)$"no longer present"

$4 \mapsto 6 \mapsto 1$ $(2\ 6\ 4\ 1\ \ldots)$All cycles covered

$1 \mapsto \mathbf{2}$ $(2\ 6\ 4\ 1)$Cycle found

$\mathbf{7} \mapsto 3$ $(7\ 3 \ldots$"no longer present"

$3 \mapsto \mathbf{7}$ $(7\ 3)$Cycle found

$$\tau = (2\ 6\ 4\ 1)(3\ 7)$$

5.18 remark. Note that when an element is not in a cycle, you can think of it as a mapping onto itself. For example , above whenever the mapping function of $(3, 7)$ took 2 or 6 it just spat them back, so actually we had $2 \mapsto 6 \mapsto 6 \mapsto 2 \mapsto 6$ etc

This also means that above when we say not present in any "to-the-left" cycles, is just the same as reaching the left-most cycle, where each function whose cycle does not contain the element, just maps it into itself until the last cycle is reached

5.19 remark. Sometimes it is useful to write a permutation as a product of transpositions, this is particularly easy from the disjoint cycle notation form

$$(2\ 6\ 4\ 1)(3\ 7) = (2\ 1)(2\ 4)(2\ 6)(3\ 7)$$

5.1 *Parity*

5.20 definition. Sign For σ written as the composite of disjoint cycles $\gamma_1, \ldots, \gamma_k$, where γ_i is an r_i cycle

$$\operatorname{sgn}(\sigma) := (-1)^{r_1-1}(-1)^{r_2-1} \cdots (-1)^{r_k-1}$$

5.21 theorem. *Let σ and τ be permutations of a finite set X. Then* $\operatorname{sgn} \sigma \circ \tau = \operatorname{sgn} \sigma \cdot \operatorname{sgn} \tau$

Note that the corollary includes not-disjoint γ

5.22 corollary. *For $\sigma = \gamma_1\gamma_2 \ldots \gamma_k$, where γ_i is a r_i-cycle ,*

$$\operatorname{sgn}(\sigma) = (-1)^{r_1-1}(-1)^{r_2-1} \ldots (-1)^{r_k-1}$$

5.23 definition. Alternating Group the subset of S_n consisting of the even permutations

5.24 notation. A_n

5.25 example.

5.26 proposition. ***Order****when a permutation is written as a composition of disjoint cycles, its order is the least common multiple of the lengths of the cycles*

6 Groups

6.1 definition. Binary Operation $f : X \times X \to X$

6.2 example. The operations of addition, subtraction and multiplication in $\mathbb{R}$

6.3 notation. $+, \times, \circ, *$ (and several more)

6.4 remark. It is important to define the set being operated on by the binary operator

6.5 example. $m * n = m^n$ is a binary operation in $\mathbb{R}$, but not in $\mathbb{Z}$.
Take $n = -1$, then we get $m^{-1} = \frac{1}{m}$, which does not satisfy the definition, since $-1 \in \mathbb{Z}$ but $\frac{1}{m} \notin \mathbb{Z}, \forall\, m \neq |1|$

6.6 definition. Group Let G be a set and let $*$ be a binary operation on G. Then, the pair $(G, *)$ is a group *iff*

1. $\forall x, y, z \in G$ we have $(x * y) * z = x * (y * z)$ `Associativity Law`
2. There is an element $e \in G$ such that $x * e = e * x = x\ \forall x \in G$ `Identity`
3. There is an element $y \in G$ such that $x * y = y * x = e\ \forall x \in G$ `Inverse`

6.7 remark. The group operation is often called *product*

6.8 remark. Usually one says that "*G is a group*", omitting the $*$

6.9 remark. In a group where the operator is understood as addition, for all x one represents the identity element by 0 and its inverse by $-x$

6.10 remark. In general, $e = 1$ and x^{-1} represents the inverse

6.11 example. Show that the pair $(\mathbb{Z}, +)$ is a group

Let $m, n \in \mathbb{Z}$. Then $n + m \in \mathbb{Z}$, so the binary operation of addition is defined on $\mathbb{Z}$. Now note that,

1. Let $p, q, r \in \mathbb{Z}$. Then, we have (p+q) + r = p + (q+r) ✓
2. $0 \in \mathbb{Z}$, such that $0 + n = n + 0 = n \forall\ n \in \mathbb{Z}$. Hence, 0 is the identity element ✓
3. Let $n \in \mathbb{Z}$. Then, $-n \in \mathbb{Z}$ and $n + (-n) = (-n) + n = 0$. hence, $-n \in \mathbb{Z}$ and $-n$ is the inverse of n ✓

Extra Fields

6.12 definition. Abelian G for which $x * y = y * x \forall\ x, y \in G$

6.13 definition. Order $|G|$

6.1 *Subgroups*

6.14 definition. Subgroup a subset H of G with satisfies the following:

1. $\forall x, y \in H$ we have $x * y = \in H$
2. $e \in H$
3. If $x \in H$, then $x^{-1} \in H$

6.15 notation. $H \leq G$, $H \subseteq G$

6.16 remark. $e_H = e_G$

6.17 remark. If $H \neq G$, then H is a *proper subgroup*

6.18 notation. $H < G$, $H \subset G$

6.19 example. $(\mathbb{Z}, +) < (\mathbb{R}, +)$

6.20 example. Show that the alternating group on n elements of A , A_n, is a subgroup of the symmetric group $(S_n, \circ)$

1. For $\sigma, \tau \in A_n$ we have that
$$\sigma\tau \in A_n \because sgn(\sigma\tau) = sgn(\sigma)\, sgn(\tau) = (1)(1) \implies \text{Even} \checkmark$$
2. $Id \in S_n$ and $sgn(Id) = 1$, since $Id = (1)(2)\dots(n)$ ✓
3. $sgn(\sigma) = 1$ and $sgn(\sigma)\, sgn(\sigma^{-1}) = sgn(Id) = 1$ ✓

7 Isometries of the Plane

7.1 *Introduction*

Vector Geometry Essentials - Revision Level 1

Generalities and Examples

7.1 definition. Isometry a transformation Φ on the plane, such that the distance between any two points remains unchanged. Formally, for $\Phi : \mathbb{R}^2 \to \mathbb{R}^2$

$$d(\Phi(P), \Phi(Q)) = d(Q, P), \quad \forall\, P, Q \in \mathbb{R}^2$$

To do. . .

□ 1 (p. 8): Read up on fields