M1J2 Summary Notes (JMC Year 1, 2017/2018 syllabus)

Fawaz Shah

(STILL UNDER CONSTRUCTION)

Dr Lawn refers to propositions, theorems, corollaries and lemmas. In this document I will refer to them all as 'theorems'.

This document contains a list of definitions and a list of theorems.

Contents

Part I

Abstract Linear Algebra

1 Definitions

2 Theorems

2.1 Vector spaces

2.2 Subspaces

2.3 Spanning sets and linear independence

2.4 Bases and dimension

2.5 Linear maps

Part II

Group Theory

3 Definitions

Binary operation A binary operation on a set G is a any function $f : G \times G \to G$

Associative A binary operation $\star$ on a set G is associative if it satisfies:

$$(a \star b) \star c = a \star (b \star c) \tag{1}$$

for all $a, b, c \in G$.

Commutative A binary operation $\star$ on a set G is commutative if it satisfies:

$$a \star b = b \star a \tag{2}$$

for all $a, b \in G$.

Left/right identity An element $e \in G$ is called the left identity if:

$$e \star g = g \tag{3}$$

for all $g \in G$. Similar statement for right identity.

(Two sided) Identity element An element $e \in G$ is a two-sided identity element if it is both a left identity and a right identity.

From now on the two-sided identity element will be referred to as e.

Left/right inverse An element $h \in G$ is called the left inverse of $g \in G$ if:

$$h \star g = e \tag{4}$$

Similar statement for right inverse.

Two sided inverse A two sided inverse of an element $g \in G$ is both a left inverse and a right inverse of g.

From now on the two-sided inverse of g will be referred to as g^{-1}.

Group A group $(G, \star)$ is a set G equipped with a binary operation $\star$ such that:

1. $\star$ is associative
2. $\star$ has an identity element in G
3. Every $g \in G$ has an inverse $g^{-1} \in G$

Order (group) The order of a group $(G, \star)$ is the size of G.

Abelian group An Abelian group is a group with a commutative binary operation $\star$.

Powers of g We can define the powers of any $g \in G$ to be:

$$g^n = \begin{cases} g \star g \star ...g & n > 0 \\ g^{-1} \star g^{-1} \star ...g^{-1} & n < 0 \\ e & n = 0 \end{cases} \tag{5}$$

where in the first cases there are n copies of g, and in the second case there are $-n$ copies of g^{-1}.

The normal exponent rules apply.

Definition of $[a]$ and $\mathbb{Z}_n$ For any $a \in \mathbb{Z}$:

$$[a] = \{b \in \mathbb{Z} \mid b \equiv a \bmod n\} \tag{6}$$

Note that $[a]$ forms an equivalence class, and there are exactly n of these equivalence classes. $\mathbb{Z}_n$ is the set of all these equivalence classes.

$$\mathbb{Z}_n = \{[0], [1]...[n-1]\} \tag{7}$$

Definition of $\mathbb{Z}_n^*$ $\mathbb{Z}_n^*$ is the set of all $[a]$ such that $[a]$ is invertible. Note in this case the identity element is $[1]$.

$$\mathbb{Z}_n^* = \{[a] \in \mathbb{Z}_n \mid \exists [b] \in Z_n \quad s.t. \quad [a] \star [b] = [1]\} \tag{8}$$

Some common choices for $\star$ are $[a] + [b] = [a+b]$ and $[a] \times [b] = [ab]$.

Order (element) The order of any $g \in G$ is the smallest positive integer such that:

$$g^n = e \tag{9}$$

Cyclic group + generator A group $(G, \star)$ is cyclic if:

$$G = \{g^n \mid n \in \mathbb{Z}\} \tag{10}$$

g is called the generator of the group.

Permutation A permutation σ on n symbols is a bijection:

$$\sigma : \{1...n\} \to \{1...n\} \tag{11}$$

Symmetric group The symmetric group S_n on n symbols is the set of all permutations of n symbols.

$$S_n = \{\sigma : \{1...n\} \to \{1...n\}\} \tag{12}$$

Note that S_n is a set of functions. Therefore the identity element is the identity function.

Cycle A permutation $\sigma \in S_n$ is a cycle if there exists some $a_1...ak \in \{1...n\}$ such that:

$$\sigma(a_1) = a_2, \quad \sigma(a_2) = a_3 \quad ... \quad \sigma(a_k) = a_1 \tag{13}$$

and $\sigma(i) = i$ for all $i \notin \{1...n\}$. k is called the length of the cycle. The notation for a cycle is $(a_1...a_k)$.

Disjoint cycles Two cycles $(a_1...a_m)$ and $(b_1...b_n)$ are disjoint if no a_i is equal to any b_j.

Subgroup Let $(G, \star)$ be a group, and $H \subseteq G$. $(H, \star)$ is a subgroup of G if:

- $e \in H$
- For any $g, h \in H$, $g \star h \in H$
- For any $g \in H$, $g^{-1} \in H$

Cyclic subgroup Let $(G, \star)$ be a group. For any $g \in G$, the cyclic subgroup $\langle g \rangle$ generated by g is defined as:

$$\langle g \rangle = (\{g^i \mid i \in \mathbb{Z}\}, \star) \tag{14}$$

Left/right cosets Let $(G, \star)$ be a group and $(H, \star)$ a subgroup. For any $g \in G$, the left coset of H by g (denoted by gH) is defined as:

$$gH = \{g \star h \mid h \in H\} \tag{15}$$

Similar definition for right coset of H by g (denoted by Hg).

The set of all left cosets of H by g is denoted by $G : H$.
The set of all right cosets of H by g is denoted by $H : G$.

4 Theorems

4.1 Groups

4.2 Modular arithmetic and $\mathbb{Z}_n$

4.3 Cyclic groups

4.4 Symmetric groups

4.5 Subgroups

4.6 Cosets and Lagrange's Theorem

Part III
Analysis

5 Definitions

Sequence A sequence is simply a map $f : \mathbb{N} \to \mathbb{R}$, denoted by a_n

Convergence (as $n \to \infty$) A sequence a_n converges to a limit L if for all real numbers $\epsilon > 0$, there exists an $N \in \mathbb{N}$ such that for all $n > N$ we have $|a_n - L| < \epsilon$.

$$\forall \epsilon > 0 \quad \exists N \in \mathbb{N} \quad s.t \quad \forall n > N \quad |a_n - L| < \epsilon \tag{16}$$

Tends to infinity (sequence) We say a sequence tends to infinity if for all $R \in \mathbb{R}$, the sequence a_n is eventually bigger than R.

$$\forall R \in \mathbb{R} \quad \exists N \in \mathbb{N} \quad s.t. \quad \forall n > N \quad a_n > R \tag{17}$$

Shift The shift of a sequence by say, k, is the sequence $b_n = a_{n+k}$

Triangle inequality The general triangle inequality is:

$$|x - y| < |x - z| + |z - y| \tag{18}$$

Setting $z = 0$ gives us:

$$|x - y| > |x| - |y| \tag{19}$$

Then setting $y = -y$ gives us the familiar case:

$$|x + y| < |x| + |y| \tag{20}$$

Bounded above A sequence a_n is bounded above if there's a real number A such that $a_n < A$ for all n.

Bounded below A sequence a_n is bounded below if there's a real number A such that $a_n > A$ for all n.

Bounded A sequence a_n is bounded if there's a real number A such that $|a_n| < A$ for all n.

Increasing A sequence is increasing if $a_{n+1} \geq a_n$ for all n.

Strictly increasing A sequence is strictly increasing if $a_{n+1} > a_n$ for all n.

Decreasing A sequence is decreasing if $a_{n+1} \leq a_n$ for all n.

Strictly decreasing A sequence is strictly decreasing if $a_{n+1} < a_n$ for all n.

Monotonic A sequence is monotonic if it is increasing or decreasing.

Supremum The supremum A of a set S is the least upper bound of that set i.e. the smallest number such that $s \leq A$ for all $s \in S$.

Supremum (function) The supremum of a function f is the sup of $\{f(x) \mid x \in \text{dom}(f)\}$.

Infimum The infimum B of a set S is the greatest lower bound of that set i.e. the largest number such that $s \geq B$ for all $s \in S$.

Infimum (function) The infimum of a function f is the inf of $\{f(x) \mid x \in \text{dom}(f)\}$.

Subsequence A subsequence of a_n is a sequence $a_{f(n)}$, where $f(n)$ is a strictly increasing function.

Cauchy sequence A sequence is Cauchy if all the terms get arbitrarily close to one another. To put it mathematically:

$$\forall \epsilon > 0 \quad \exists N \in \mathbb{N} \quad s.t \quad \forall m, n \geq N \quad |a_n - a_m| < \epsilon \tag{21}$$

Partial sum The n^{th} partial sum S_n of a sequence a_n is the sum of terms up to that point:

$$S_n = \sum_{i=1}^{n} a_n \tag{22}$$

Summable A sequence is summable if the sequence of its partial sums converges. The limit of the sequence of partial sums will be:

$$L = \sum_{i=1}^{\infty} a_n \tag{23}$$

Absolutely summable A sequence a_n is absolutely summable if $|a_n|$ is summable.

Conditionally summable A sequence is conditionally summable if it is summable but not absolutely summable.

Power series The power series associated with a sequence a_n is the sequence of partial sums:

$$\sum_{i=1}^{n} a_i x^i \tag{24}$$

Radius of convergence The radius of convergence R of a power series $P(x)$ is defined as the largest x for which $P(x)$ is convergent.

$$R = sup\{x \in \mathbb{R} \mid P(x) \text{ convergent}\} \tag{25}$$

Limit as $x \to \infty$ (function) A function $f(x)$ tends to a limit L as $x \to \infty$ if for all real numbers $\epsilon > 0$, there exists an $R \in \mathbb{R}$ such that for all $x \geq R$ we have $|f(x) - L| < \epsilon$.

$$\forall \epsilon > 0 \quad \exists R \in \mathbb{R} \quad s.t \quad \forall x > R \quad |f(x) - L| < \epsilon \tag{26}$$

Tends to infinity (function) A function $f(x)$ tends to infinity as $x \to \infty$ if for any $M \in \mathbb{R}$ there exists an $R \in \mathbb{R}$ such that if $x > M$ then $f(x) > R$.

$$\forall M \in \mathbb{R} \quad \exists R \in \mathbb{R} \quad s.t. \quad x > M \Rightarrow f(x) > R \tag{27}$$

One-sided limit A function $f(x)$ tends to a limit L as $x \to a^-$ if for any $\epsilon > 0$ there exists a $\delta > 0$ such that if $x \in (a - \delta, a)$ then $|f(x) - L| < \epsilon$.

$$\forall \epsilon > 0 \quad \exists \delta > 0 \quad s.t. \quad x \in (a - \delta, a) \Rightarrow |f(x) - L| < \epsilon \tag{28}$$

Same format for the other sided limit ($x \to a^+$)
(Note that $\epsilon - \delta$ definition is only used for limits as x tends to a finite number a, not infinity)

Limit as $x \to a$ A function $f(x)$ tends to a limit L as $x \to a$ if we have both:

$$\lim_{x \to a^-} f(x) = L \quad \text{and} \quad \lim_{x \to a^+} f(x) = L \tag{29}$$

Limit as $x \to a$ (ϵ - δ def.) A function $f(x)$ tends to a limit L as $x \to a$ if:

$$\forall \epsilon > 0 \quad \exists \delta > 0 \quad s.t. \quad |x - a| < \delta \Rightarrow |f(x) - L| < \epsilon \tag{30}$$

Continuous A function $f(x)$ is continuous at a if:

$$\lim_{x \to a} f(x) = f(a) \tag{31}$$

Continuous (ϵ - δ def.) A function $f(x)$ is continuous at a if for all $\epsilon > 0$ there is a $\delta > 0$ such that if $|x - a| < \delta$ then $|f(x) - f(a)| < \epsilon$.

$$\forall \epsilon > 0 \quad \exists \delta > 0 \quad s.t. \quad |x - a| < \delta \Rightarrow |f(x) - f(a)| < \epsilon \tag{32}$$

Continuous everywhere A function $f(x)$ is continuous everywhere if it is continuous at a for all $a \in \text{dom}(f)$.

Open interval An open inteval I is a set $I \subseteq \mathbb{R}$ of the form:

- $I = (a, b)$ for some $a, b \in \mathbb{R}$, or
- $I = (-\infty, b)$, or
- $I = (a, +\infty)$, or
- $I = \mathbb{R}$

Discontinuity Discontinuity is the negation of continuity. Hence a function $f(x)$ is discontinuous at a if there exists $\epsilon > 0$ such that for all $\delta > 0$, $|x - a| < \delta$ AND $|f(x) - f(a)| > \epsilon$.

$$\exists \epsilon > 0 \quad s.t. \quad \forall \delta > 0 \quad |x - a| < \delta \text{ AND } |f(x) - f(a)| > \epsilon \tag{33}$$

Bounded (function) A function $f(x)$ is bounded if the set of all possible values of f(x) is bounded.

Differentiable (ver. 1) A function $f(x)$ is differentiable at a if:

$$\lim_{x \to a} \frac{f(x) - f(a)}{x - a} \tag{34}$$

exists.

Differentiable (ver. 2) A function $f(x)$ is differentiable at a if:

$$\lim_{h \to 0} \frac{f(a + h) - f(a)}{h} \tag{35}$$

exists.

Differentiable everywhere A function $f(x)$ is differentiable everywhere if it is differentiable at a for all $a \in \text{dom}(f)$.

Global maximum A function $f(x)$ has a global maximum at a if $f(a) \geq f(x)$ for all other values of $f(x)$.

Similar definition for global minimum.

Local maximum A function $f(x)$ has a local maximum at a if $f(a) \geq f(x)$ for all x in the set $(a - \epsilon, a + \epsilon)$, for some ϵ.

Similar definition for local minimum.

Lipschitz continuous A function is Lipschitz continuous if:

$$|f'(x)| \leq L \Rightarrow |f(x_1) - f(x_2)| \leq L|x_1 - x_2| \tag{36}$$

6 Theorems

6.1 Sequences

Every convergent sequence has a unique limit.

Every convergent sequence is bounded.

If all terms of a convergent sequence are larger than a number B, then so is its limit.

Some properties of limits:

$$\lim_{x\to\infty}(a_n + b_n) = \lim_{x\to\infty} a_n + \lim_{x\to\infty} b_n \tag{37}$$

$$\lim_{x\to\infty}(\lambda a_n) = \lambda \lim_{x\to\infty} a_n \tag{38}$$

$$\lim_{x\to\infty}(a_n b_n) = \lim_{x\to\infty} a_n \lim_{x\to\infty} b_n \tag{39}$$

$$\lim_{x\to\infty}(\frac{a_n}{b_n}) = \frac{\lim_{x\to\infty} a_n}{\lim_{x\to\infty} b_n} \tag{40}$$

where λ is any real number.

If $a_n \to \infty$ and b_n is bounded below, $a_n + b_n \to \infty$.

If $a_n \to \infty$ and b_n is bounded below by a positive number, $a_n b_n \to \infty$.

If a_n is bounded and $b_n \to \infty$, then $\frac{a_n}{b_n} \to 0$.

If $a_n \to \infty$, for any real number λ:

- $\lambda < 0 \Rightarrow \lambda a_n \to -\infty$
- $\lambda = 0 \Rightarrow \lambda a_n \to 0$
- $\lambda > 0 \Rightarrow \lambda a_n \to \infty$

If $a_n \to a$ and $b_n \to b$, and for all n $a_n < b_n$, then $a < b$.

Sandwich Theorem
If $a_n \leq b_n \leq c_n$ for all n, and a_n and c_n tend to the same limit L, then $b_n \to L$.

Every bounded monotonic sequence is convergent.

Completeness Axiom
Every non-empty subset of the real numbers which is bounded above has a supremum. Similar statement for infimum.

Useful results for sequences:

$$\lim_{n\to\infty} \lambda^n = \begin{cases} \infty & \lambda > 1 \\ 1 & \lambda = 1 \\ 0 & -1 < \lambda < 1 \end{cases} \tag{41}$$

λ^n diverges if $\lambda = -1$.

If $m > 0$ and $\lambda > 1$ then $\frac{\lambda^n}{n^m} \to \infty$ (exponentials beat powers).

If $m > 0$ then $\frac{\log(n)}{n^m} \to 0$ (powers beat logs).

6.2 Subsequences

If $a_n \to L$ then any subsequence $a_{f(n)} \to L$.

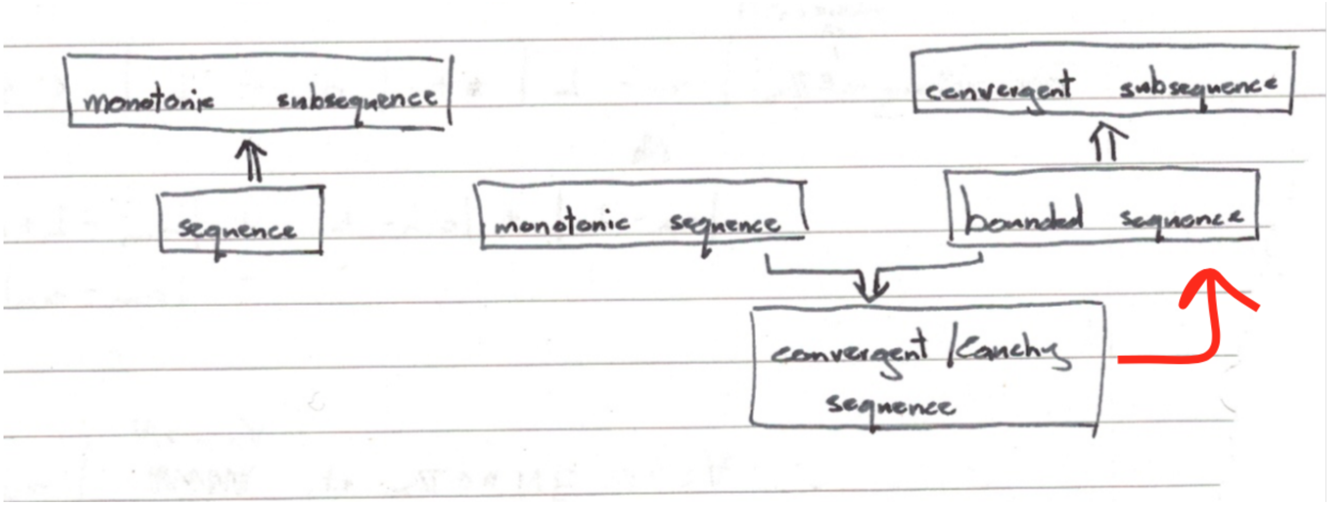
If two subsequences of a_n converge to different limits, a_n doesn't converge to a limit.

Every sequence has a monotonic subsequence.

Bolzano-Weierstrass Theorem
Every bounded sequence has a convergent subsequence.

Every Cauchy sequence is bounded.

Cauchy sequence $\Leftrightarrow$ convergent sequence (for real numbers).



6.3 Summability

A sequence is summable iff the sequence of its partial sums converges.

If two subsequences of a sequence a_n converge to two different limits, a_n is not summable.

If a_n and b_n are summable with $\sum_{i=0}^{\infty} a_i = a$ and $\sum_{i=0}^{\infty} b_i = b$:

- $a_n + b_n$ is summable with $\sum_{i=0}^{\infty}(a_i + b_i) = a + b$.
- λa_n is summable with $\sum_{i=0}^{\infty} \lambda a_i = \lambda a$ (for any real number λ)

If $b_n = a_{n+k}$ then a_n summable $\Leftrightarrow$ b_n summable.

a_n is summable $\Rightarrow a_n \to 0$.

Let S_n denote the sequence of partial sums of a_n ($S_n = \sum_{i=0}^{n} a_n$). A sequence of non-negative numbers a_n is summable iff S_n is bounded above. Similar statement for sequences of non-positive numbers.

Every absolutely summable sequence is summable.

Comparison test
If $b_n > a_n$ for all n then b_n summable $\Rightarrow$ a_n summable.

Alternating series test
If a_n is a decreasing sequence AND $a_n \geq 0$ for all n AND $a_n \to 0$ then $(-1)^{n+1}a_n$ is a convergent sequence.

Ratio test for sequences
Let $r = \lim_{n\to\infty} \frac{a_{n+1}}{a_n}$:

- $r < 1 \Rightarrow a_n$ is absolutely summable
- $r > 1 \Rightarrow a_n$ is not summable
- $r = 1$ is an indeterminate case

6.4 Power series

The power series associated with a sequence a_n converges iff the sequence of partial sums of $a_n x^n$ converges (i.e. if $\sum_{i=0}^{n} a_i x^i$ converges).

Let $P(x)$ be a power series. If $P(a)$ converges absolutely for some a, then $P(x)$ converges absolutely for all x such that $|x| < |a|$

Let R be the radius of convergence of $P(x)$. For all real numbers a:

- $|a| < R \Rightarrow P(a)$ converges absolutely
- $|a| > R \Rightarrow P(a)$ diverges

Ratio test for power series
Let $r = \frac{a_{n+1}}{a_n}$. Let $P(x) = \sum_{i=0}^{n} a_i x^i$ (i.e. the power series associated with a_n):

- $r \to 0 \Rightarrow R = \infty$
- $r \to L$ for some $L \Rightarrow R = \frac{1}{L}$
- $r \to \infty \Rightarrow R = 0$

Note: if $r = 1$ here then $R = 1$. This is DIFFERENT to the ratio test for sequences, where $r = 1$ is an indeterminate case.

6.5 Continuity

The limit of a function at any specific point is unique.

If functions f and g are continuous at a:

- $(f + g)$ is continuous at a
- fg is continuous at a
- $\frac{1}{f(x)} and \frac{1}{g(x)}$ are continuous at a
- $g \circ f$ is continuous at a

Any polynomial in $\mathbb{R}$ is continuous

Any rational function in $\mathbb{R}$ is continuous

Sequential continuity
A function f is continuous at a iff $f(a_n) \to f(a)$ for all sequences a_n such that $a_n \to a$.

Any continuous function on a closed bounded interval is bounded.

Intermediate Value Theorem
If f continuous and $f(a) \leq f(b)$ for some a, b, then there exists some $c \in [a, b]$ such that $f(a) \leq f(c) \leq f(b)$.

Fixed Point Theorem
If f continuous and $f : [a, b] \to [a, b]$, then there exists some $c \in [a, b]$ such that $f(c) = c$.

Polynomials of odd degree have at least 1 root.

f differentiable $\Rightarrow$ f continuous.

6.6 Differentiable functions

If functions f and g are differentiable at a:

- $(f + g)$ is differentiable at a
- fg is differentiable at a

- $\frac{1}{f(x)} and \frac{1}{g(x)}$ are differentiable at a
- $g \circ f$ is differentiable at a
- g^{-1} and f^{-1} are differentiable at a

Let f be continuous and differentiable. If f has a local extremum at a then $f'(a) = 0$ (except at endpoints of the interval).

Let f be continuous and differentiable. If f has a local extremum at c (say in the interval $[a, b]$), there are 3 possiblities:

- c is an endpoint of $[a, b]$
- $f'(c) = 0$
- c is a non-differentiable point

Mean Value Theorem
Let f be continuous on $[a, b]$ and differentiable on (a, b). There exists a point $c \in (a, b)$ such that:

$$f'(c) = \frac{f(b) - f(a)}{b - a} \tag{42}$$

Rolle's Theorem
Let f be continuous and differentiable on (a, b). If $f(a) = f(b)$ then there exists some $c \in (a, b)$ such that $f'(c) = 0$. This is a special case of the Mean Value Theorem.