

M1F Summary Notes

JMC Year 1, 2017/2018 syllabus

Fawaz Shah

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

Note that the exam will probably require you to PROVE some of these theorems, so you should refer back to the original notes for the proofs.

Boxes cover content in more detail. Titles of some theorems are given in italics.

Contents

1	Definitions	2
2	Theorems	4
2.1	Logic and Sets	4
2.2	Complex numbers	4
2.3	Proofs and Induction	6
2.4	Number Theory	6
2.5	Modular arithmetic	9
2.6	Equivalence relations and functions	10
2.7	Combinatorics	10

1 Definitions

Arbitrary union We can define the arbitrary union

$$\bigcup_{i \in I} X_i \quad (1)$$

to be the union of all sets X_i .

Arbitrary intersection We can define the arbitrary intersection

$$\bigcap_{i \in I} X_i \quad (2)$$

to be the intersection of all sets X_i .

Modulus (complex number) The modulus of $z = x + iy$ is defined as:

$$|z| = \sqrt{x^2 + y^2} \quad (3)$$

Argument (complex number) The argument of $z = x + iy$ is defined as:

$$\arg(z) = \arctan\left(\frac{y}{x}\right) \quad (4)$$

Fundamental Theorem of Algebra If a polynomial is of degree n then it has n roots in the complex plane.

Rational A number is rational if it can be expressed in the form $\frac{p}{q}$, where $p, q \in \mathbb{Z}$ and $\gcd(p, q) = 1$.

Root of unity Any z that is a solution to $z^n = 1$.

"Dense" A set S is dense in T if for any $t_1, t_2 \in T$ there exists an $s \in S$ such that $t_1 < s < t_2$

Supremum A real number b is the sup (least upper bound) of a set S if:

- every $s \in S$ is less than b (i.e. b is an upper bound)
- b is less than every other upper bound of S

Infimum A real number b is the inf (greatest lower bound) of a set S if:

- every $s \in S$ is greater than b (i.e. b is a lower bound)
- b is greater than every other lower bound of S

Bounded above A set is bounded above if it has an upper bound.

Bounded below A set is bounded below if it has a lower bound.

Coprime We say two integers a and b are coprime if $\gcd(a, b) = 1$.

Fundamental Theorem of Arithmetic Every integer greater than 1 can be expressed as a unique product of primes.

\equiv (**congruence operator**) We say $a \equiv b \pmod{m}$ if $(a - b)$ is a multiple of m .

Binary relation A binary relation \sim on a set S is a mapping satisfying $S \times S \rightarrow \text{Bool}$.

Reflexive A binary relation \sim is reflexive if for any $a \in S$:

$$a \sim a \tag{5}$$

Symmetric A binary relation \sim is symmetric if:

$$a \sim b \Leftrightarrow b \sim a \tag{6}$$

Transitive A binary relation \sim is transitive if:

$$a \sim b \wedge b \sim c \Rightarrow a \sim c \tag{7}$$

Equivalence relation A binary relation \sim is an equivalence relation iff it is reflexive, symmetric and transitive.

Equivalence class The equivalence class of $b \in S$ is the set of all $s \in S$ such that $b \sim s$.

Image The image of a function $f : A \rightarrow B$ is the set of all $b \in B$ such that $b = f(a)$ for some $a \in A$.

Injective A function $f : A \rightarrow B$ is injective if every $b \in B$ has at MOST one $a \in A$ that maps to it. Mathematically:

$$\forall x, y \in A \quad f(x) = f(y) \Rightarrow x = y \quad (8)$$

Surjective A function $f : A \rightarrow B$ is surjective if every $b \in B$ has at LEAST one $a \in A$ that maps to it. Mathematically:

$$\forall b \in B \quad \exists a \in A \quad s.t. \quad f(a) = b \quad (9)$$

Bijjective A function $f : A \rightarrow B$ is bijective iff it is both surjective and injective.

(Two-sided) inverse function The inverse of a function $f : A \rightarrow B$ is defined as $f^{-1} : B \rightarrow A$, and satisfies:

$$f^{-1} \circ f \equiv f \circ f^{-1} \equiv Id_A \quad (10)$$

Power set The power set of S is the set of all subsets of S .

Countably infinite An infinitely-sized set S is countably infinite if there exists a bijection $f : \mathbb{Z}_{>0} \rightarrow S$.

2 Theorems

2.1 Logic and Sets

Contrapositive law

For any Boolean statements P, Q :

$$(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P) \quad (11)$$

To negate any logical statements, we can flip the \forall and \exists signs and negate the predicate (the mathematical statement at the end).

2.2 Complex numbers

Complex numbers can be added, subtracted, multiplied and divided.

For any complex number z ,

$$z\bar{z} = |z|^2 \quad (12)$$

For any complex numbers z_1, z_2 :

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2} \quad (13)$$

$$\overline{z_1 - z_2} = \overline{z_1} - \overline{z_2} \quad (14)$$

$$\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2} \quad (15)$$

$$\overline{\left(\frac{z_1}{z_2}\right)} = \frac{\overline{(z_1)}}{\overline{(z_2)}} \quad (16)$$

$$\overline{(z_1)^n} = (\overline{z_1})^n \quad (17)$$

The inverse of a complex number z is such that:

$$zz^{-1} = 1 \quad (18)$$

Any complex number z can be represented in exponential form:

$$z = re^{i\theta} \quad (19)$$

where r is the modulus of z and θ is the argument.

Euler's formula

$$e^{i\theta} = \cos(\theta) + i \sin(\theta) \quad (20)$$

This can be proven using power series.

De Moivre's Theorem

For any complex number z :

$$z^n = r^n(\cos(n\theta) + i \sin(n\theta)) \quad (21)$$

This can be proven by induction or using Euler's formula.

Fundamental Theorem of Algebra

Any polynomial of degree n has n roots in the complex plane.

Roots of unity

Any root of unity (i.e. a solution to $z^n = 1$) can be expressed in the form:

$$z = e^{\frac{2\pi ki}{n}}, \quad k \in \mathbb{Z}_{\geq 0} \quad (22)$$

If we let:

$$\omega = e^{\frac{2\pi i}{n}} \quad (23)$$

then all the n^{th} roots of unity can be expressed in the form:

$$z = 1, \omega, \omega^2, \omega^3 \dots \omega^{n-1} \quad (24)$$

In general, all n^{th} roots of a complex number a can be expressed as:

$$z = a, a\omega, a\omega^2, a\omega^3 \dots a\omega^{n-1} \quad (25)$$

2.3 Proofs and Induction

Counterexample

This involves disproving a statement by providing an example situation where the statement is false.

Proof by contradiction

Assume the statement is true and reach a contradiction. This means the statement must be false.

Weak induction

If we take P as a predicate:

$$P(0) \wedge (P(k) \Rightarrow P(k+1)) \Rightarrow P(n) \quad (\forall n) \quad (26)$$

Note that we do not have to start at 0:

$$P(m) \wedge (P(k) \Rightarrow P(k+1)) \Rightarrow P(n) \quad (\forall n \geq m) \quad (27)$$

Strong induction

If we take P as a predicate:

$$P(0) \wedge ((\forall j \leq k P(j)) \Rightarrow P(k+1)) \Rightarrow P(n) \quad (\forall n) \quad (28)$$

Note that we do not have to start at 0:

$$P(m) \wedge ((\forall j \leq k P(j)) \Rightarrow P(k+1)) \Rightarrow P(n) \quad (\forall n \geq m) \quad (29)$$

We must prove $P(k) \Rightarrow P(k+1)$ for weak induction.

We must prove $(\forall j \leq k P(j)) \Rightarrow P(k+1)$ for strong induction.

Strong induction is mathematically equivalent to weak induction.

2.4 Number Theory

There is no smallest positive real number.

There always exists a real n^{th} root of a real number (for $n \in \mathbb{Z}_{>0}$).

The sum/product of any two rational numbers is rational.

The sum of a rational number and an irrational number is irrational.
(proof by contradiction)

There are infinitely many irrational numbers.
(consider $x_n = \sqrt{2} + n$ for $n \in \mathbb{Z}$)

\mathbb{Z} is unbounded in \mathbb{R} (i.e. for any real number there is always an integer larger than it).

\mathbb{Q} is dense in \mathbb{R} .

$\mathbb{R} \setminus \mathbb{Q}$ (i.e. the set of irrationals) is dense in \mathbb{R} .

Completeness Axiom

A set S has a least upper bound (sup) iff:

- S is non-empty
- S is bounded above

Corresponding statement for greatest lower bound (inf).

Every real number has a decimal expansion.

Assume for simplicity that we have a single digit real number.
Let d_n be the sequence of digits and e_n the sequence of error terms, such that $\forall n \ 0 \leq e_n \leq 1$. We have:

$$x = d_0.d_1d_2d_3\ldots \quad (30)$$

Then we can produce the digits by the following steps:

$$x = d_0 + e_0 \quad (31)$$

$$10e_0 = d_1 + e_1 \quad (32)$$

$$10e_1 = d_2 + e_2 \quad (33)$$

$$\vdots \quad (34)$$

$$10e_{n-1} = d_n + e_n \quad (35)$$

A number is rational \Leftrightarrow it has a periodic decimal expansion.

Any integer a has a quotient and remainder when divided by an integer b .
(proof by induction on a)

This quotient and remainder are unique for any a .
(proof by contradiction)

For any $x \in \mathbb{Z}_{\geq 0}$ and $\lambda, \mu \in \mathbb{Z}$, $(x \mid a)$ and $(x \mid b) \Rightarrow (x \mid \lambda a + \mu b)$.
($x \mid a$ means "x divides a")

For any $x \in \mathbb{Z}_{\geq 0}$, $(x \mid a)$ and $(x \mid b) \Rightarrow (x \mid \gcd(a, b))$.

If $(x \mid ab)$ but $\gcd(a, x) = 1$ then $(x \mid b)$.
(use Bezout's Theorem on $\gcd(a, x) = 1$)

Note: In general, $\gcd(a, b) = 1$ doesn't mean that $(a \nmid b)$, or vice versa.

The only time that $\gcd(a, b) = 1 \Leftrightarrow (a \nmid b)$ is if one of a, b are prime. This is because (take p prime) the only way for $\gcd(a, p) \neq 1$ would be if a is a multiple of p , in which case $(p \mid a)$.

Euclid's Algorithm

To find the \gcd of a and b where $a > b$. Write:

$$a = q_1 b + r_1 \tag{36}$$

$$b = q_2 r_1 + r_2 \tag{37}$$

$$r_1 = q_3 r_2 + r_3 \tag{38}$$

$$\vdots \tag{39}$$

$$r_{n-2} = q_n r_{n-1} + r_n \tag{40}$$

Continue until $r_n = 0$, return r_{n-1} .

In Haskell notation, Euclid's algorithm is specified by:

```
gcd(a, 0) = 0
gcd(a, b) = gcd(b, a mod b)
```

Bezout's Theorem

$$\gcd(a, b) = \lambda a + \mu b \quad (\text{for some } \lambda, \mu \in \mathbb{R}) \tag{41}$$

(proof by induction)

We can write a and b as:

$$a = \alpha \gcd(a, b) \quad (42)$$

$$b = \beta \gcd(a, b) \quad (43)$$

In general the solution to equation 41 is given by:

$$\gcd(a, b) = (\lambda + \beta n)a + (\mu - \alpha n)b \quad (44)$$

noting that the extra terms will always cancel out. So we have a set of solutions (λ_n, μ_n) , where:

$$\lambda_n = \lambda + \beta n, \quad \mu_n = \mu - \alpha n \quad (45)$$

If a prime $p \mid a_1 a_2 \dots a_n$ for $a_i \in \mathbb{Z}$, then p divides any of the a_i .
(proof by induction on n)

Every integer larger than 1 can be written as a product of primes.
(proof using strong induction)

Fundamental Theorem of Arithmetic

Every integer larger than 1 can be written UNIQUELY as a product of primes.
i.e. every such integer can be written as a product of primes $p_i^{x_i}$, where each p_i is distinct and every $x_i > 0$.
(proof not needed)

2.5 Modular arithmetic

$(\equiv \text{ mod } m)$ is an equivalence relation.

If $a \equiv b \text{ mod } m$ and $c \equiv d \text{ mod } m$:

$$a + c \equiv b + d \text{ mod } m \quad (46)$$

$$a - c \equiv b - d \text{ mod } m \quad (47)$$

$$ac \equiv bd \text{ mod } m \quad (48)$$

If $a \equiv b \text{ mod } m$, then for any n :

$$a^n \equiv b^n \text{ mod } m \quad (49)$$

(proof by induction)

Fermat's Little Theorem

For any prime p and $a \in \mathbb{Z}$:

$$a^p \equiv a \pmod{p} \quad (50)$$

(can be proven by induction)

Also, if a is not a multiple of p :

$$a^{p-1} \equiv 1 \pmod{p} \quad (51)$$

In the case a is a multiple of p , we can easily see $a^{p-1} \equiv 0 \pmod{p}$.

2.6 Equivalence relations and functions

A binary relation \sim is an equivalence relation iff it is reflexive, symmetric and transitive.

The equivalence class of $b \in S$ is the set of all $s \in S$ such that $b \sim s$.

The set of equivalence classes of a set S form a partition of S . In other words, each equivalence class is a disjoint subset of S .

A function has an inverse iff it is a bijection.

If f and g are injective, so is $g \circ f$.

If f and g are surjective, so is $g \circ f$.

If f and g are bijective, so is $g \circ f$.

If we define $X \sim Y$ as "there exists a bijection $f : X \rightarrow Y$ ", then \sim is an equivalence relation.

Let $P(A)$ denote the power set of a set A .

There exists no bijection $A \rightarrow P(A)$.

Examples of countably finite/infinite sets

\mathbb{Z}, \mathbb{Q} are countably infinite.

$\mathbb{R}, \mathbb{C}, \mathbb{R} \setminus \mathbb{Q}$ (set of all irrationals) are uncountably infinite.

2.7 Combinatorics

Multiplicative principle

In any n -stage process, where the r^{th} stage can be completed in a_r ways, the total

number of ways of completing the process is:

$$\prod_{r=0}^n a_r \quad (52)$$

i.e. just multiply the number of options together.

Multinomials

When expanding $(a + b + c + \dots)^n$, with r terms inside the brackets, the general term of any coefficient is $a^\alpha b^\beta c^\gamma \dots$, where $\alpha + \beta + \gamma + \dots = n$.

The coefficient in the expansion for any term $a^\alpha b^\beta c^\gamma \dots$ is given by:

$$\binom{n}{\alpha, \beta, \gamma, \dots} = \frac{n!}{\alpha! \beta! \gamma! \dots} \quad (53)$$

Note if we set $r = 2$ in the above equation we get the familiar binomial coefficient:

$$\binom{n}{\alpha, \beta} = \frac{n!}{\alpha! \beta!} \quad (54)$$

$$= \frac{n!}{\alpha! (n - \alpha)!} \quad (55)$$

since $\beta = n - \alpha$.