M1F Summary Notes (JMC Year 1, 2017/2018 syllabus)

Fawaz Shah

UNDER CONSTRUCTION

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.

Contents

1 Definitions

Arbitrary union We can define the arbitrary union

$$\bigcup_{i \in I} X_i \tag{1}$$

to be the union of all sets X_i.

Arbitrary intersection We can define the arbitrary intersection

$$\bigcap_{i \in I} X_i \tag{2}$$

to be the intersection of all sets X_i.

Modulus (complex number)

Argument (complex number)

2 Theorems

2.1 Logic and Sets

Contrapositive law

$$(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P) \tag{3}$$

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,

$$z\overline{z} = |z|^2 \tag{4}$$

For any complex numbers z_1, z_2:

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2} \tag{5}$$
$$\overline{z_1 - z_2} = \overline{z_1} - \overline{z_2} \tag{6}$$
$$\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2} \tag{7}$$
$$\overline{(\frac{z_1}{z_2})} = \frac{\overline{(z_1)}}{\overline{(z_2)}} \tag{8}$$
$$\overline{(z_1)^n} = (\overline{z_1})^n \tag{9}$$

The inverse of a complex number z is such that:

$$zz^{-1} = 1 \tag{10}$$

Any complex number z can be represented in exponential form:

$$z = re^{i\theta} \tag{11}$$

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

Euler's formula

$$e^{i\theta} = \cos(\theta) + i\sin(\theta) \tag{12}$$

This can be proven using power series.

De Moivre's Theorem
For any complex number z:

$$z^n = r^n(\cos(n\theta) + i\sin(n\theta)) \tag{13}$$

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:

$$z = e^{\frac{2\pi ki}{n}}, \quad k \in \mathbb{Z}_{\geq 0} \tag{14}$$

2.3 Number theory

Weak induction
If we take P as a predicate:

$$P(0) \wedge (P(k) \Rightarrow P(k+1)) \Rightarrow P(n) \quad (\forall n) \tag{15}$$

Note that we do not have to start at 0:

$$P(m) \wedge (P(k) \Rightarrow P(k+1)) \Rightarrow P(n) \quad (\forall n \geq m) \tag{16}$$

Strong induction
If we take P as a predicate:

$$P(0) \wedge ((\forall j \leq k \ P(j)) \Rightarrow P(k+1)) \Rightarrow P(n) \quad (\forall n) \tag{17}$$

Note that we do not have to start at 0:

$$P(m) \wedge ((\forall j \leq k \ P(j)) \Rightarrow P(k+1)) \Rightarrow P(n) \quad (\forall n \geq m) \tag{18}$$

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.

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.

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

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

Euclid's Algorithm
To find the *gcd* of a and b where $a > b$. Write:

$$a = q_1 b + r_1 \tag{19}$$
$$b = q_2 r_1 + r_2 \tag{20}$$
$$r_1 = q_3 r_2 + r_3 \tag{21}$$
$$\vdots \tag{22}$$
$$r_{n-1} = q_n r_{n-1} + r_n \tag{23}$$

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

In Haskell notation:

$\text{gcd}(a, 0) = 0$
$\text{gcd}(a, b) = \text{gcd}(b, a \bmod b)$

Bezout's Theorem

$$\text{gcd}(a, b) = \lambda a + \mu b \quad (\text{for some } \lambda, \mu \in \mathbb{R}) \tag{24}$$

We can write a and b as:

$$a = \alpha \,\text{gcd}(a, b) \tag{25}$$
$$b = \beta \,\text{gcd}(a, b) \tag{26}$$

In general the solution to equation 24 is given by:

$$\text{gcd}(a, b) = (\lambda + \beta n)a + (\mu - \alpha n)b \tag{27}$$

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

$$\lambda_n = \lambda + \beta n, \quad \mu_n = \mu - \alpha n \tag{28}$$

Every integer larger than 1 can be written as a product of primes. (use strong induction to prove)

Fundamental Theorem of Arithmetic
Every integer larger than 1 can be written UNIQUELY as a product of primes. (proof not needed)

2.4 Equivalence relations and functions

2.5 Combinatorics