Discrete Mathematics (SEF015)

What is "Discrete Mathematics"?

discrete: consisting of distinct, differentiated parts

- Discrete Mathematics is the branch of Mathematics dealing with questions involving finite or countably infinite sets (usually).
- The numbers involved are usually integers or fractions (rational numbers)
- Discrete Maths describes processes consisting of a sequence of individual steps; Calculus (by contrast) describes "continuously" changing processes. Discrete Maths lends itself to applications involving computers

Some remarks about Mathematics

- Mathematics deals with statements
- Often these statements are about numbers
- These statements are true or false
- Deciding whether a statement is true or false requires proof.

Basic Tools: Numbers, sets and functions.

The Integers.

Some basic sets (collections of elements)

$\mathbb{N}$ (natural numbers)

used to count the number of an object

Consists of $0, 1, 2, 3, 4, \ldots$

Also called the non-negative numbers.

Also given the notation $\mathbb{N}_0$.

The collection $\mathbb{N}^+$ consists of $1, 2, 3, 4, \ldots$ (excluding 0), and is the set of positive integers

NB Some people exclude 0 from $\mathbb{N}$ but I always include it (so $\mathbb{N} = \mathbb{N}_0$ in this module). Note that $\mathbb{N}_0$ always contains 0 while $\mathbb{N}^+$ does not)

$\mathbb{Z}$ (the integers)

$\mathbb{Z}$: German Zahlen - numbers

Consists of $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$

Discrete (gaps between consecutive integers)

$\mathbb{Q}$ (the rationals)

Consists of all expressions of the form $\frac{a}{b}$ where a and b are integers with $b \neq 0$. We have $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$.

[There are unique integers c, d with $d > 0$ such that $\frac{a}{b} = \frac{c}{d}$ and c, d have no common integer divisor greater than 1. This is the lowest terms expression of $\frac{a}{b}$]

$\frac{c}{d}$

$\mathbb{R}$ (the real numbers) [VERY INFORMAL]

includes numbers such as $-2, 1, \pi, \sqrt{2}$ and all decimal numbers (terminating or not; recurring or not).

In fact, every real number has an expression as a decimal number.

NOTE. All of these definitions are very informal, especially the last one (for $\mathbb{R}$). Proper formal definitions for these sets is beyond the scope of this course.

Properties of the integers [CHAT PAGE]

I'll presume you are familiar with addition, subtraction, multiplication (and division) on $(\mathbb{N},)\ \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, as formal definitions are hard.

For $\mathbb{Q}$ we have $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$, $\frac{a}{b}-\frac{c}{d}=\frac{ad-bc}{bd}$

$\frac{a}{b}\times\frac{c}{d}=\frac{ac}{bd}$ and $\frac{a}{b}\div\frac{c}{d}=\frac{ad}{bc}$ ($b,d\neq 0$, $c\neq 0$ in last one)

Also if $\frac{a'}{b'}=\frac{a}{b}$ & $\frac{c'}{d'}=\frac{c}{d}$ then $\frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'}$,

$\frac{a'}{b'}-\frac{c'}{d'}=\frac{a}{b}-\frac{c}{d}$ and $\frac{a'}{b'}\times\frac{c'}{d'}=\frac{a}{b}\times\frac{c}{d}$.

Note that subtraction isn't always defined for $\mathbb{N}$ and division is not always defined for $\mathbb{N}$ and $\mathbb{Z}$, and division by 0 is never defined.

For example, $3-6$ is not a natural number

$5\div 2$ is not an integer.

Properties of the integers.

(These also apply to the rational numbers and real numbers)

[YOU MUST REPLACE EVERY OCCURENCE OF "INTEGER"]

(A0) For all integers a, b, the quantity $a+b$ is an integer. (closure of addition)

(A1) For all integers a, b, c we have $(a+b)+c = a+(b+c)$. (associativity of addition)

(A2) For all integers a, b we have $a+b = b+a$. (commutativity of addition)

(A3) There exists an integer 0 such that for all integers a we have $a+0 = 0+a = a$. (existence of additive identity [namely 0])

(A4) For all integers a there is an integer $-a$ such that $a+(-a) = (-a)+a = 0$. (existence of additive inverses)

$-a$ "minus a"

$-a$ is the negative of a

(M0) For all integers a, b the quantity ab (or $a \cdot b$ or $a \times b$) is an integer (closure of multiplication)

(M1) For all integers a, b, c we have $(ab)c = a(bc)$. (associativity of multiplication)

(M2) For all integers a, b we have $ab = ba$. (commutativity of multiplication)

(M3) There exists an integer 1 such that for all integers a we have $a \cdot 1 = 1 \cdot a = a$. (existence of multiplicative identity [namely 1])

(D) For all integers a, b, c we have

$$a(b+c) = (ab) + (ac)$$
$$(a+b)c = (ac) + (bc).$$

(distributive laws)

NOTE. The identity elements 0 and 1 are unique. And for each a, its negative $-a$ is unique. (So is a^{-1} [see below] whenever this exists.)

NEXT PAGE

SOME

Properties of $\mathbb{Z}$ deducible from the above

For all integers a, b

- $0 \cdot a = a \cdot 0 = 0$
- $-(-a) = a$
- $-a = (-1) \cdot a = a \cdot (-1)$
- $(-a)(-b) = ab$
- $(-a)b = a(-b) = -(ab)$
- $-(a+b) = (-a) + (-b)$

Subtraction

For all a, b we define $a-b$ as $a+(-b)$.

$a+(-b)+(-c)$

We have $a-(b+c)=(a-b)-c$, $a-(-b)=a+b$, $b-a=-(a-b)$ and $a-(b-c)=a-b+c$ for all a, b, c.

[Also $a(b-c)=ab-ac$, $(a-b)c=ac-bc$.]

Integer subtraction is NOT associative. Eg $(3-2)-2=1-2=-1\neq 3=3-(2-2)$ and NOT commutative. Eg $3-2=1\neq -1=2-3$

Nor is there an -ive identity.

[We have $a-0=a$ for all a, but there is no integer b such that $b-a=a$ for all integers a.]

Further properties of $\mathbb{Q}$ and $\mathbb{R}$

In $\mathbb{Q}$ and $\mathbb{R}$ we also have

(M4) For all $a\neq 0$ there is an element a^{-1} such that $a\cdot a^{-1}=a^{-1}\cdot a=1$. [MULT INVERSE]

a^{-1} is the inverse of a, and is unique.

In $\mathbb{Z}$ only 1 & -1 have inverses. For example 2 has no inverse in $\mathbb{Z}$. In $\mathbb{Q}$, $2^{-1}=\frac{1}{2}$.

DIVN Have $\frac{a}{b}$ or a/b or $a\div b$ defined as ab^{-1} whenever $b\neq 0$.

Properties include $(a^{-1})^{-1}=a$ for all $a\neq 0$, and $(ab)^{-1}=b^{-1}a^{-1}$ for all nonzero a, b.

More sophisticated operations / properties

Absolute value. For a in $\mathbb{Z}$ (or $\mathbb{Q}$ or $\mathbb{R}$) the absolute value or modulus of a is defined to be

$$|a| = \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0 \end{cases}$$

eg
$|3| = 3$
$|-4| = 4$

Note that $|a|$ is always non-negative.

Division "Algorithm"

If $b \neq 0$ then for all integers a there exist integers q (quotient) and r (remainder) such that (i) $a = q \cdot b + r$ & (ii) $|r| < |b|$.

If we insist that $0 \leq r < |b|$ $\left(\text{or } -\frac{|b|}{2} < r \leq \frac{|b|}{2}\right)$ then q and r are unique.

Examples.

- $a = 13$, $b = 3$ implies that $q = 4$, $r = 1$ since $13 = 4 \cdot 3 + 1$
- $a = 17$, $b = -5$ implies that $q = -3$, $r = 2$ since $17 = (-3)(-5) + 2$
- $a = -1$, $b = 4$ implies that $q = -1$, $r = 3$ since $-1 = (-1) \cdot 4 + 3$
- $a = 5$, $b = 3$ implies that $q = 1$, $r = 2$ since $5 = 1 \cdot 3 + 2$

[If we have $-\frac{|b|}{2} < r \leq \frac{|b|}{2}$, the last two become $q = 0$, $r = -1$ (from the relation $-1 = (0)4 + (-1)$) and $q = 2$, $r = -1$ (from $5 = 2 \cdot 3 + (-1)$)]

Definition. Let a, b be integers. We say that a *divides* b, and write $a \mid b$, if there is an integer c such that $ac = b$.

Properties.
- $a \mid b$ implies $a \mid nb$ for all integers n
- $a \mid b$ and $a \mid c$ implies that $a \mid (b+c)$ (& $a \mid (b-c)$)
- $a \mid b$ and $b \mid c$ implies that $a \mid c$

Non-property $a \mid b$ and $z \mid b$ does not imply that $(a+z) \mid b$. If we take $a=1, b=2, z=2$ then $a \mid b$, $z \mid b$ but $(a+z) \nmid b$ (this is $3 \nmid 2$)

Definition Let a, b be integers. We say that a is a divisor of b if $a \mid b$.

Definition An integer p is *prime* if p is at least 2 and the only positive divisors of p are 1 and itself. If m is an integer at least 2, and it is not prime then m is composite.

1 is neither prime nor composite.

Smallest primes 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ...

(There are infinitely many primes, so we cannot list all of them.)

Fundamental Theorem of Arithmetic

Thm Each positive integer can be written as a product of primes, and this expression is unique up to ordering of those primes.

Examples $12 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2 = 2 \cdot 2 \cdot 3$

$10 = 2 \cdot 5 = 5 \cdot 2$

1 = empty product. (no prime factors)

NB The number of times each prime occurs in the factorisation is invariant. Allowing 1 to be prime destroys the uniqueness for we could then have $6 = 2 \cdot 3 = 3 \cdot 2 \cdot 1 = 1 \cdot 2 \cdot 1 \cdot 3 =$ ---etc.

Extension to $\mathbb{Z}$ Each non-zero integer can be expressed as the product of a sign [unit], namely $+1$ or -1, and some primes. The expression is unique up to ordering of the primes.

Examples.

- $8 = 1 \cdot 2 \cdot 2 \cdot 2$ → primes.
- $-5 = -1 \cdot 5$
- $-1 = -1$ (no primes here)

sign

Question Are there any other mathematical objects with similar properties?

Yes! (Certain types of) polynomials.

Polynomials

Definition A polynomial is an expression of the form

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

where $a_0, \ldots, a_n$ are the coefficients of f and x is a dummy variable (a place holder)

[NOTE: f is NOT a function.]

- f is an integer polynomial (or polynomial over $\mathbb{Z}$) if $a_0, \ldots, a_n$ belong to $\mathbb{Z}$
  The set of all integer polynomials is denoted $\mathbb{Z}[x]$.
- f is a polynomial over $\mathbb{Q}$ if $a_0, \ldots, a_n$ belong to $\mathbb{Q}$
  The set of all such polynomials is denoted $\mathbb{Q}[x]$.
  [This should be the same as rational polynomial, but this term is sometimes wrongly confused with rational function]
- f is a real polynomial (polynomial over $\mathbb{Q}$) if $a_0, \ldots, a_n$ belong to $\mathbb{R}$ The set of all real polynomials is denoted

Defn In the above, if $a_n \neq 0$ then f is said to have **degree** n.
We write $\deg f = n$.
The **zero polynomial** (with $a_i = 0$ for all i) does not have a degree.

Sometimes the degree of the zero polynomial is assigned the special symbol $-\infty$, having various properties suggested by this notation.

Examples

- 0 (zero polynomial) — degree undefined (as far as this module is concerned)
- 5 (a non-zero constant polynomial) — degree 0
- $2+5x$ (a linear polynomial) — degree 1
- $-1+2x+5x^2$, $-3+0\cdot x+4x^2$ (quadratic polynomials) — degree 2

Note An expression such as $x+2x^2+3x^3+\cdots$ with an infinite number of terms (the $a_i x^i$ with $a_i \neq 0$) is NOT a polynomial.
Polynomials only have a finite number of terms

Interlude: Summation and Product notation

Consider a list of n objects $a_1, \to a_n$ (which live in some object with the usual rules of arithmetic).

We can write

$$a_1 + a_2 + \cdots + a_n = \sum_{i=1}^{n} a_i$$

The index i is a dummy variable, and so it can be replaced by another letter (but not n, which is not dummy).

Thus $\sum_{i=1}^{n} a_i = \sum_{j=1}^{n} a_j = \sum_{k=1}^{n} a_k$.

$\Sigma, \sigma/\varsigma$ Greek Sigma (s)

But $\sum_{n=1}^{n} a_n$ MAKES NO SENSE.

For products we have

$$a_1 \cdot a_2 \cdot a_3 \cdot \cdots \cdot a_n = \prod_{i=1}^{n} a_i = \prod_{k=1}^{n} a_k$$

Π, π Greek Pi (p)

Empty Sum (the case $n=0$, a sum of 0 terms)

$$\sum_{i=1}^{0} a_i = 0 \qquad \left(\sum_{i=1}^{1} a_i = a_1, \ \sum_{i=1}^{2} a_i = a_1 + a_2 \text{ etc}\right)$$

Empty product (the case $n=0$, a product of 0 terms)

$$\prod_{i=1}^{0} a_i = 1 \qquad \left(\prod_{i=1}^{1} a_i = a_1, \ \prod_{i=1}^{2} a_i = a_1 a_2, \text{ etc}\right)$$

Note Some people like to refer to infinite sums and products, but there are no such things. In reality, the entities referred to in this way are something completely different.

Back to polynomials

Thus $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ can be written as $\sum_{i=0}^{n} a_i x^i$

starts at 0, so n+1 "summands"

(but strictly we shouldn't be thinking of this as a sum in this context.)

Equality of polynomials

The polynomials $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$ are equal if and only if

$a_0 = b_0$, $a_1 = b_1$, $a_2 = b_2$, ... etc.

That is if and only if $a_i = b_i$ for all i in $\mathbb{N}$.

(We let $a_i = 0$ if $i > n$ and $b_i = 0$ if $i > m$.)

Note that this notion of equality only depends on the coefficients of the polynomials. [AND NOT THE dummy variables]

Thus $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(y) = \sum_{i=0}^{n} a_i y^i$ are considered to be equal (as elements of $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$)

But if there are multivariate polynomials in two variables labelled x & y then

$f(x,y) = \sum_{i=0}^{n} a_i x^i$ and $g(x,y) = \sum_{i=0}^{n} a_i y^i$ are NOT equal

note the difference.

Operations on polynomials

Let $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$

To simplify the exposition, assume that $a_i = 0$ if $i > n$ and $b_i = 0$ if $i > m$.

The definitions of addition, subtraction and multiplication of polynomials are motivated by assuming that the dummy variable x is an actual number and manipulating accordingly

ADDITION & SUBTRACTION

We have $f(x)+g(x) = \sum_{i=0}^{N} (a_i+b_i)x^i$

and $f(x)-g(x) = \sum_{i=0}^{N} (a_i-b_i)x^i$

where $N = \max(n,m) = \begin{cases} n & \text{if } n \geq m \\ m & \text{if } n < m \end{cases}$

MULTIPLICATION

Motivated by $(a_i x^i)(b_j x^j) = a_i b_j x^{i+j}$

We have $f(x)g(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n+m} x^{n+m}$

$$= \sum_{i=0}^{n+m} c_i x^i$$

where $c_k = \sum_{i=0}^{k} a_i b_{k-i}$ (coeff of x^k)

$= a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0$ for all k.

Thus $f(x)g(x) = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k$

PROPERTIES

For polynomials (over $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$) we have the same properties of their arithmetic as polynomials over $\mathbb{Z}_n$, that is properties (A0)–(A4), (M0)–(M3), (D) hold. [SEE EARLIER]

So for all polynomials $f(x), g(x), h(x)$ we have

$f(x)(g(x)+h(x)) = f(x)g(x) + f(x)h(x)$

$f(x)(g(x)h(x)) = (f(x)g(x))h(x)$

$f(x)+g(x) = g(x)+h(x)$, and so on.

Some examples. Let $f(x) = 1+2x+3x^2$, $g(x) = 4+5x^2$

Then $f(x)+g(x) = (1+2x+3x^2)+(4+5x^2) = 5+2x+8x^2$

$f(x)-g(x) = (1+2x+3x^2)-(4+5x^2) = -3+2x-2x^2$

$$f(x)\cdot g(x) = (1)(4)+((1)(0)+(2)(4))x+(1\cdot5+2\cdot0+3\cdot4)x^2 + (1\cdot0+2\cdot5+3\cdot0+0\cdot4)x^3+(1\cdot0+2\cdot0+3\cdot5+0\cdot0+0\cdot4)x^4$$

$$= 4+8x+17x^2+10x^3+15x^4$$

Alternative working.

$$f(x)\cdot g(x) = (1+2x+3x^2)4+(1+2x+3x^2)5x$$
$$= 4+8x+12x^2+5x^2+10x^3+15x^4$$
$$= 4+8x+17x^2+10x^3+15x^4$$

Proof that $f(x)+g(x) = g(x)+f(x)$

$$f(x)+g(x) = \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i = \sum_{i=0}^{N} (a_i+b_i)x^i$$

$N = \max(n,m)$

$$= \sum_{i=0}^{N} (b_i+a_i)x^i$$ [Commutativity of addition in $\mathbb{Z}/\mathbb{Q}/\mathbb{R}$]

$$= \sum_{i=0}^{m} b_i x^i + \sum_{i=0}^{n} a_i x^i = g(x)+f(x).$$

Some properties such as associativity of polynomial addition are also easy to verify. Other properties such as associativity of multiplication are harder.

Binomial Law.

A useful fact to remember is that for (all) numbers a and b we have [a, b in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$]

$$(a+b)^2 = a^2 + 2ab + b^2,$$
$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3,$$
$$(a+b)^4 = a$$

In general, the coëfficients of $(a+b)^n$ are given by the n^{th} row of Pascal's Triangle

		1				row 0
	1		1			row 1
1		2		1		row 2
	1		3		1	row 3
1		4		6		4		1	row 4
	1		5		10		10		5		1	row 5

Each entry is the sum of the two entries above it, except for the top 1.
[The rows can be extended infinitely in both directions by adding zeroes].