Misc

Misc

- $\cos(a+b)+i\sin(a+b) = e^{i(a+b)} = [\cos(a)+i\sin(a)][\cos(b)+i\sin(b)] = \cos(a)\cos(b) - \sin(a)\sin(b) + i[\cos(a)\sin(b) + \cos(b)\sin(a)]$
  - $\cos(2\theta)=\cos^2(\theta) - \sin^2(\theta)$
  - $\sin(2\theta)=2\cos(\theta)\sin(\theta)$
- $\sin(\pi - x) \equiv \sin(x)$
- $\cos(-x) \equiv \cos(x)$
- $\sin(x \pm \pi) \equiv -\sin(x)$
- $\cos(x \pm \pi) \equiv -\cos(x)$
- $\tan(x \pm \pi) \equiv \tan(x)$
- Something that was inside a trig function (eg 2x in sin(2x)) should <u>not</u> be simplified further until all solutions have been found — adjust the range instead

Number systems

Bases

- **Base conversion: Divide by the new base, record the remainder, then repeat with the quotient, once you have have a quotient of 0 stop and write the number left-to-right using the remainders <u>bottom-to-top</u>**
- **If a divides b, then to convert between base a and b it suffices to convert each digit to/from b and concatenate the results**

Euclid’s division algorithm

```
divide(a, b)
    r := a
    q := 0
    while r >= b
        r -= b
        q++
    //a = qb + r (a/b gives quotient q and remainder r)
    return (q, r)
```

Greatest common divisor

```
gcd(m, n)
    assert m >= 0 && n >= 0
    // Or just assert ordering
    if m > n
        m, n = n, m
    if m == 0
        return n
    return gcd(n mod m, m)
```

- This works because if d divides n=qm+r then d divides qm and r

Modular arithmetic

- a and b are congruent mod n ⇔ ∃k ∈ ℤ: a=b+kn ⇔ n divides a−b
- **If x mod n = a and y mod n = b:**
  - **x+y mod n = a + b mod n**
  - **xy mod n = ab mod n**
    - x^k mod n = a^k mod n
  - **x−y mod n = a − b mod n**
  - **Division is complicated**
  - *z^{xy} mod n = $(z^x \text{ mod } n)^y$ mod n*
- *Fermat's little theorem: For all integers n and p, if p is prime and n and p are coprime, then n^{p-1} mod p = 1*
- Interpreting an n-bit two's complement number x as unsigned gives x mod 2^N — the above is why normal arithmetic works with two's complement

Sets of numbers

Subsets of the reals

- $x \in \mathbb{Q} \Leftrightarrow \exists m \in \mathbb{Z}: \exists n \in \mathbb{N} \backslash \{0\}: z = m/m$, and m and n are coprime
- **x is algebraic iff <u>x is real and</u> there exists a finite polynomial with rational (or equivalently integer) coefficients with a root x**
- **x is transcendental iff <u>it is real and</u> it is not algebraic**

The real numbers: Axioms

- **Commutativity of addition and multiplication**
- **Associativity of addition and multiplication**
- **Distributivity of multiplication over addition**
- **Existence of additive identity 0**
- **Existence of multiplicative identity 1**
- **0 and 1 are distinct**
- All the above hold for the naturals also
- Existence of additive inverse: $\forall x.\ \exists -x: x+(-x) = 0$
- All the above hold for the integers also
- Existence of multiplicative inverse: $\forall x.\ \exists x^{-1}: x \cdot (x^{-1}) = 1$
- All the above hold for the rationals and algebraics also
- Transitivity: $\forall x, y, z.\ (x<y \land y<z) \Rightarrow x<z$
- Trichotomy: **For all x, y; exactly one of these is true: x<y, y<x, x=y**
- Preservation of ordering under addition: $\forall x, y, z.\ x<y \Rightarrow x+z<y+z$
- Preservation of ordering under multiplication: $\forall x, y, z.\ (x<y \land 0<z) \Rightarrow x \cdot z<y \cdot z$
- **Completeness: Every non-empty subset that has an upper bound has a least upper bound in the reals**

The real numbers: Completeness

- **Let $S \subseteq \mathbb{R}$, $S \neq \varnothing$, and $\leq$ be the standard total ordering over $\mathbb{R}$**
  - **u $\in \mathbb{R}$ is a upper bound of S iff $\forall x \in S.\ x \leq u$**
  - **S is bounded iff there exists an upper bound of S**
  - **u $\in \mathbb{R}$ is the least upper bound (supremum) of S iff it is the least element of the set of upper bounds of S** (for all upper bounds u', u≤u')
- *There are dual notions of lower bound, greatest lower bound, and infimum*
- **Theorem (Archimedean property of the reals): $\forall a, b \in \mathbb{R}_{>0}.\ \exists n \in \mathbb{N}: na > b$**

  Proof: Assume for the sake of contradiction that there exists positive reals a, b such that for all natural n $na \leq b$

  Then, b is an upper bound of $\{na : n \in \mathbb{N}\}$

  By the completeness of the reals, there exists a supremum l of $\{na : n \in \mathbb{N}\}$

  Hence, $\forall n \in \mathbb{N}.\ na \leq l$

  Hence, $\forall n \in \mathbb{N}.\ (n+1)a \leq l$. So, $\forall n \in \mathbb{N}.\ na \leq l-a$

  Hence, $l-a$ is an upper bound. As a is positive, $l-a<l$. Hence, there exists an upper bound smaller than the supremum?!

Complex numbers

- $(a+bi)(c+di)=ac-bd+(ad+bc)i$
- If $z=a+bi$, z^* (can also be denoted by an overbar) $=a-bi$
  - $(z+w)^* = z^* + w^*$
  - $\mathbf{(zw)^* = z^*w^*}$
    - $(z/w)^*=z^*/w^*$
- **If $z=re^{i\theta}$, then $z=r[\cos(\theta) + i\cdot\sin(\theta)]$** and $z^*=re^{-i\theta}$
  - If $z=x+iy$, $r^2=x^2+y^2$ and $\tan(\theta)=y/x$
  - <u>θ is measured anticlockwise</u> from the real axis — <u>a diagram is necessary</u> to establish the relationship between $\arctan(y/x)$ and θ
- To evaluate z_1/z_2 multiply top and bottom by z^*_2 to obtain $z_1/z_2=(z_1z_2^*)/((|z_2|)^2)$
- $|z_1z_2|=|z_1||z_2|$
- Triangle inequality: $\mathbf{|z_1+z_2| \leq |z_1| + |z_2|}$
- $\mathbf{||z| - |w|| \leq |z-w|}$
- **Fundamental theorem of algebra: Every polynomial of degree n has exactly n** (not necessarily distinct) **roots in $\mathbb{C}$**

Vectors

Vectors

- Vectors u and v are equal iff their components are equal iff they have the same length and are parallel and in the same direction
- If a and b are position vectors, then c=a+b is the position vector s.t. OACB is a parallelogram or equivalently is the point obtained by top and tailing a and b
- **Pythagoras extends to higher dimensions — $|(a_1, \ldots, a_n)|^2$ = sum of (a_i^2)**
- **$(a_1, \ldots, a_n)\cdot(b_1, \ldots, b_n)$** = sum of (a_ib_i) **= $|a||b|\cos(\theta)$** where θ is angle between a and b

  Proof for n=2: Let α be the angle made between a and the origin and β be the angle made between b and the origin. Without loss of generality, assume α≤β. Then, θ=β − α.
  Thus, $\cos(\theta)=\cos(\beta)\cos(\alpha) + \sin(\beta)\sin(\alpha) = (b_1/|b|)(a_1/|a|) + (b_2/|b|)(a_2/|a|) = a_1b_1/|a||b| + a_2b_2/|a||b|$.

  So, $a_1b_1+a_2b_2=|a||b|\cos(\theta)$
- a and b are orthogonal (perpendicular) iff $a\cdot b = 0$
- $|\lambda v|=\lambda|v|$

Subspaces

- **span({u_1, …, u_m}) =** $\{a_1u_1+\ldots+a_mu_m: a_1, \ldots, a_m \in \mathbb{R}\}$ = **the set of all linear combinations of u_1, …, u_m**
  - **Equivalently span({u_1, …, u_m}) = the vector $a_1u_1+\ldots+a_mu_m$ where a_1, …, a_m are** real **parameters**
- **A finite subset S of $\mathbb{R}^n$ is a subspace of $\mathbb{R}^n$ iff S is: non-empty, closed under addition (u, v ∈ S ⇒ u+v ∈ S), and closed under scalar multiplication (u ∈ S and λ ∈ ℝ ⇒ λu ∈ S)**
  - Equivalently, S is a subspace of $\mathbb{R}^n$ iff $S \subseteq \mathbb{R}^n$ and S = span(S) ≠ ∅
    - Hence, if S is a non-empty finite subset of $\mathbb{R}^n$, then span(S) is a subspace of $\mathbb{R}^n$
  - Due to closure under scalar multiplication, every subspace of $\mathbb{R}^n$ contains the zero vector

Linear independence

- **$\{u_1, \ldots, u_m\}$ is linearly dependent** iff a vector can be written as a linear combination of the others **iff there is a linear combination with coefficients not all zero that gives the zero vector**
- **$\{u_1, \ldots, u_m\}$ is linearly independent iff it is not linear dependent iff (if a linear combination gives the zero vector then the coefficients are all zero)**

Bases

- **A set of vectors U is a basis of a subspace S iff U is linearly independent and span(U)=S**
- **If V={v_1, …, v_m} spans S, then any linearly independent subset of S contains at most m vectors**
- Any two bases of the same subspace have the same number of elements
  Proof: Let U={u_1, …, u_m} and W={w_1, …, w_p} be bases for S
  As U spans S and W is a linearly independent subset of S, $m \leq p$
  As W spans S and U is a linearly independent subset of S, $p \leq m$
  Thus, p=m
- Dimension of a subspace = cardinality of any basis for the subspace
- If $U \subseteq S$ and $|U| > \dim(S)$, then U is linearly dependent

Matrices

Misc

- **A matrix of order mxn has m rows and n columns**
- **a_{ij} is the element in the ith row and jth column**
- **A matrix is diagonal iff every element not on the leading diagonal is zero** (elements on leading diagonal may also be zero)
    - Matrix multiplication of diagonal matrices reduces to element wise multiplication
    - *Determinant of a diagonal matrix = product of elements along diagonal*
- Matrix multiplication is associative
- Matrix multiplication distributes over matrix addition
- A^T is the transpose of A — the rows of A^T are the columns of A and the columns of A^T are the rows of A
    - $(AB)^T \equiv B^T A^T$
    - $(A+B)^T \equiv A^T + B^T \equiv B^T + A^T$ as matrix addition is commutative
- **If C=AB, the element in row i and column j of C is the dot product of row i of A and column j of B** — row, row, row your boat down the column fall
- <u>Can either pre-multiply a matrix to both sides or post-multiply a matrix to both sides — can not place it wherever is convenient</u>
- $(ABC\ldots)^{-1} = \ldots C^{-1} B^{-1} A^{-1}$

Row operations

- **The elementary row operations are: Swap two rows, multiply a row by a non-zero real, add a non-zero real multiple of a row to another**
- A ~ B (A and B are row equivalent) iff A can be transformed to B using a series of elementary row operations
- Each elementary row operation can be written as pre-multiplication by a(n invertible) matrix
- A matrix is in row-echelon form iff the first non-zero entry in each row is further right than the first non-zero entry in the previous row
- Creating an augmented matrix by including the RHS then reducing to row echelon form simplifies a system of simultaneous equations

Row operations and the determinant

- **Swapping two rows causes the sign of the determinant to flip**

  Proof sketch: Induction on n. Base case n=2. Inductive step, calculate determinant using a row that wasn't in the swap

- **Add a multiple of a row to another has no impact on the determinant**

  Proof sketch: Corresponding matrix can fairly easily be shown to have det = 1 (as **a matrix with non-zero elements only on the diagonal has det = product of diagonal elements**)

  - Corollary: A row is a multiple of another ⇒ determinant = 0

- **Multiplying a row (or a column) by a constant k increases the determinant by a factor of k**

  Proof: Trivial

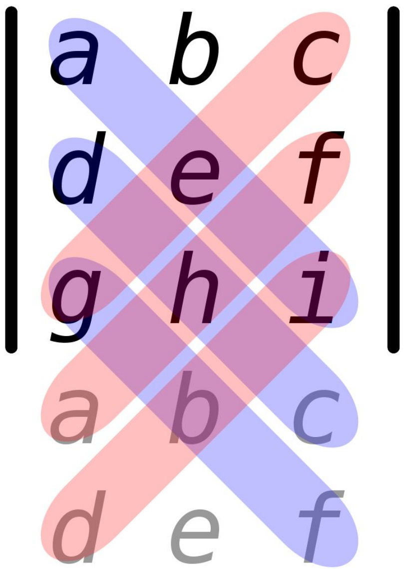
Matrix inverse: Row operations

- **Theorem: If a series of elementary row operations transforms a (square) matrix A into I, then A is invertible and the same sequence transforms I into A^{-1}**
  Proof: We have that $E_n \ldots E_1 A = I$. Let $E = E_n \ldots E_1$
  As E is a product of invertible matrices, it is invertible
  $AE = IAE = E^{-1}EAE = E^{-1}IE = I$
  So, $A^{-1}AE = A^{-1}I$ and thus $E = A^{-1}$
- Augmenting a matrix by including the identity matrix then carrying out row operations to turn it into the identity matrix causes the augmented part to become the inverse

Determinant of a 3x3 matrix: The rule of Sarrus

- <u>Only works for 3x3</u>

1. Write out the first 2 rows again below the matrix
2. Working your way down the left hand column, sum the products of the (first 3 elements of the) leading diagonals
3. Working your way down the right hand column, sum the products of the (first 3 elements of the) trailing diagonals
4. Determinant = sum of leading diagonals − sum of trailing diagonals



Matrix inverse: Cofactors

$$\begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix}$$

Multiply the minor by +1 or −1 accordingly to find the cofactor

1. **Create a new matrix C where each element is the cofactor of that element in the original matrix**
2. **Write down C^T**
3. **Write down the determinant of the original matrix**
4. **Inverse = $1/|\text{original}| \times C^T$**

Linear independence of vectors

- **A set of n vectors is linearly independent iff the matrix it is the column vectors of has non-zero determinant**
  Proof sketch: Linearly independent iff Ua = 0 doesn't have any solutions other than a=0 where U is the matrix, a is the vector of coefficients, and 0 is the zero vector
  Only solution is a=0 iff U is invertible iff U has non-zero determinant

Linear transformations and coordinates

- **A function T: $\mathbb{R}^m \mapsto \mathbb{R}^n$ is a linear transform iff it preserves addition (T(u+v) ≡T(u)+T(v)) and preserves scalar multiplication (T(λu)≡λT(u))**
  - Hence, must map zero vector to itself
- **Theorem: A function is a linear transform iff it can be written as multiplication by a matrix**
  Proof sketch: Matrix multiplication distributes over addition and preserves scalar multiplication
- **Coordinates of a vector v with respect to a basis B = vector of coefficients of linear combination of B that gives v**
- **To construct a matrix from a linear transform T: Pick bases for $\mathbb{R}^m$ and $\mathbb{R}^n$ V={v_1, …, v_m} and W={w_1, …, w_n} and let the i^{th} column be the coordinates of T(v_i) with respect to W**
- **A transition matrix (and its inverse) allows conversion between coordinates in two bases for the same subspace**
- **Transition matrix = matrix for linear transform using identity function**

Eigenvectors

- $\underline{v}$ is an eigenvector of M ⇔ $M\underline{v} = \lambda\underline{v}$ where λ is a scalar constant (the eigenvalue)
  - $M\underline{v} = \lambda\underline{v} \Leftrightarrow IM\underline{v} = I\lambda\underline{v} \Leftrightarrow IM\underline{v} - I\lambda\underline{v} = 0 \Leftrightarrow (M - I\lambda)\underline{v} = 0$
- **To find eigenvalues: Solve $\det(M - \lambda I) = 0$ for λ**
- **To find eigenvector sub in λ and solve $M\underline{v} = \lambda\underline{v}$ for $\underline{v}$**
- **<u>A root in the eigenvalue equation that is repeated n times could have up to n non-parallel eigenvectors associated with it</u>**
- **<u>If there are non-real solutions, include them</u>**
- *Sum of the leading diagonal of a matrix ≡ sum of its eigenvalues — this is a useful check*
- *Product of eigenvalues ≡ det(M) — this is a useful check*

Diagonalisation

- An nxn matrix is diagonalisable ⇔ it has n non-parallel eigenvectors
- **Let V be the matrix where each column is an eigenvector of M. Let D the diagonal matrix of eigenvalues for the eigenvectors in the corresponding columns in U.**
  Then, $V^{-1}MV=D$
  - **Corollary: $VDV^{-1}=M$ and thus $M^k=VD^kV^{-1}$**

Sequences

Convergent sequences

- **Sequence a_n converges to l** ($a_n \to l$) **iff $\forall \varepsilon \in \mathbb{R}_{>0}. \exists N \in \mathbb{N}: \forall n \in \mathbb{N}_{>N}. |a_n - l| < \varepsilon$**
  - **To prove: Construct a suitable N in terms of epsilon** and show this provides a sufficient condition
- **If a_n converges to l, then every subsequence of a_n also converges to l**
  - **Contrapositive: If there exists a subsequence of a_n that does not converge to l, then a_n does not converge to l**
    - **Corollary: If there exists a pair of subsequences that converge to different limits, then a_n is divergent**
  - Subsequence = a sequence (of infinitely many terms) obtained by removing some terms without adding any
- **Squeeze rule: If a_n and b_n both converge to the same limit l and $\exists N \in \mathbb{N}: \forall n \in \mathbb{N}{>}N.\ a_n \leq c_n \leq b_n$, then c_n also converges to l**
- **If a_n, b_n, c_n converge to A, B, C respectively:**
  - $|a_n| \to A$
  - $\lambda a_n \to \lambda A$
  - $a_n + b_n \to A+B$
  - $a_n b_n \to AB$
  - $1/a_n \to 1/A$

Properties of sequences

- **a_n diverges** (to (positive) infinity) **iff $\forall K \in \mathbb{R}.\ \exists N \in \mathbb{N}: \forall n \in \mathbb{N}_{>N}.\ a_n > K$**
- a_n is decreasing iff $\forall n \in \mathbb{N}.\ a_n \geq a_{n+1}$
- a_n is increasing iff $\forall n \in \mathbb{N}.\ a_n \leq a_{n+1}$
- **a_n is bounded above iff $\exists U \in \mathbb{R}.\ \forall n \in \mathbb{N}.\ a_n \leq U$**
- **a_n is bounded below iff $\exists U \in \mathbb{R}.\ \forall n \in \mathbb{N}.\ L \leq a_n$**
- **a_n is bounded iff it is bounded above and below**
- **If a_n is convergent, then it is bounded**
- **If a_n is increasing and bounded above, then it is convergent**
- **If a_n is decreasing and bounded below, then it is convergent**
- **a_n oscillates iff it is neither convergent nor divergent**

Asymptotics

- **$a_n \in O(b_n)$ iff $\exists\, c, N \in \mathbb{R}: \forall n \in \mathbb{N}_{>N}\ [|a_n| \leq c|b_n|]$** — b_n is an asymptotic upper bound for a_n
- **$a_n \in \Omega(b_n)$ iff $\exists\, c, N \in \mathbb{R}: \forall n \in \mathbb{N}_{>N}\ [|a_n| \geq c|b_n|]$** — b_n is an asymptotic lower bound for a_n
- **$a_n \in \Theta(b_n)$ iff $a_n \in O(b_n)$ and $a_n \in \Omega(b_n)$**

- **A useful trick: $[f(n)]^k + [f(n)]^{k-1} + \dots + [f(n)]^0 \leq [f(n)]^k + \dots + [f(n)]^k$ if $f(n) \geq 1$**
  E.g. $n^2+2n+1 \in O(n^2)$ as $n^2+2n+1 \leq n^2+2n^2+n^2$ (for $n>1$) $= 4n^2$

Recurrence relations

- The homogeneous second-order linear recurrence $ax_n + bx_{n-1} + cx_{n-2}=0$ has auxiliary equation $a\lambda^2+b\lambda+c=0$
  - **If auxiliary equation has distinct roots r_1, r_2: $x_n=Ar_1^n+Br_2^n$**
  - **If auxiliary equation has repeated root r: $x_n=Ar^n+Bnr^n$**
  - A and B are found using initial conditions
- The homogeneous second-order linear recurrence $ax_n + bx_{n-1} + cx_{n-2}=f(n)$ is solved by solving the homogeneous case and adding a particular solution **$p(n)$ s.t. $ap(n)+bp(n-1)+cp(n-2) \equiv f(n)$**
  - If f(n) is a kth degree polynomial, use a general kth degree of polynomial in n as p(n)
    - *Multiply p(n) through by n if a root of auxiliary equation is 1 — multiply through by n^2 if 1 is a repeated root*

Series

Series

- **sum from i=0 to i=∞ of a_i converges to t iff the sequence of partial sums s_n = sum from i=0 to i=n of a_i converges to t**
- **a_n converges to 0 is necessary but not sufficient for Σa_n converges**
- **$\Sigma|a_n|$ is sufficient but not necessary for Σa_n converges**
- **If Σa_n and Σb_n converge to S and T:**
    - **$\lambda\Sigma a_n \to \lambda S$**
    - **$\Sigma a_n+b_n \to S+T$**
- **Comparison test: If Σb_n converges and $\exists N \in \mathbb{N}: \forall n \in \mathbb{N}_{>N}. 0 \le a_n \le b_n$, then a_n also converges**
    - **Contrapositive: If Σa_n diverges and $\exists N \in \mathbb{N}: \forall n \in \mathbb{N}_{>N}. 0 \le a_n \le b_n$, then b_n also diverges**
    - It is not a coincidence that this looks a lot like the squeeze rule
- **Ratio test: Let $|a_{n+1}/a_n| \to k$, then:**
    - **$0 \le k < 1 \Rightarrow \Sigma a_n$ converges**
    - **k>1** (including ratio diverges) **$\Rightarrow \Sigma a_n$ diverges**
    - **<u>k=1</u> ⇒** was a waste of time, **<u>can't tell anything</u>**

Power series

- **A power series is a series of the form $\Sigma a_n x^n$**
- **Theorem: If $\exists R \in \mathbb{R}_{\geq 0}$: $\Sigma a_n R^n$ converges then, $\forall x \in \mathbb{R}$ [$|x|<R \Rightarrow \Sigma a_n x^n$ converges]**
  - **The largest such R is called the radius of convergence — for $|x|<R$ $\Sigma a_n x^n$ converges and for $|x|>R$ $\Sigma a_n x^n$ diverges** — behaviour at $x=\pm R$ is indeterminate
    - **Ratio test is a good way of finding**
- Let $f(x) = \Sigma a_n x^n$ and $g(x) = \Sigma b_n x^n$ have domains $|x|<R_1$ and $|x|<R_2$ where R_1 and R_2 are the radii of convergence. Let $R=\min(R_1, R_2)$. Then for all $|x|<R$:
  - If $f(x)=g(x)$, then $a_n=b_n$ for all n
  - **$f(x)+g(x) = \Sigma(a_n+b_n)x^n$**
  - $\lambda f(x) = \Sigma \lambda a_n x^n$
  - **$f(x)g(x) = \Sigma(a_0 b_n+a_1 b_{n-1}+\ldots+a_n b_0)x^n$**
  - These are useful when considering Taylor series
- **Binomial theorem: $\Sigma(qCn)x^n$ converges to $(1+x)^q$ with radius of convergence $|x|<1$**

Long division

- Let $s/t \in (0; 1)$:
  - $r_0=10s$
  - $q_{i+1} = r_i$ div t
  - $r_{i+1} = 10(r_i \bmod t)$
  - $s/t=\Sigma q_i/10^i$ starting at $i=1$ up to $i=\inf$ (or equivalently up to i s.t. $r_i=0$)
  - For a finite approximation: $s/t=q_1/10^1+\ldots+q_n/10^n$ $(+\ r_n/t10^{n+1})$

Calculus

Limits

Limits

- Let f be a function with domain of I or I\{a}
  - **$\lim_{x \to a-} = l$ iff for every sequence x_n in I s.t. $x_n \to a$ and x_n is bounded above by a, the sequence $f(x_n) \to l$**
  - **$\lim_{x \to a+} = l$ iff for every sequence x_n in I s.t. $x_n \to a$ and x_n is bounded below by a, the sequence $f(x_n) \to l$**
  - **$\lim_{x \to a} = l$ iff for every sequence x_n in I s.t. $x_n \to a$ and x_n does not contain a, the sequence $f(x_n) \to l$**
    - **$\lim_{x \to a} = l$ iff $\lim_{x \to a-} = l$ and $\lim_{x \to a+} = l$**
- **Same rules apply as for convergent sequences**

Continuity

- **f is continuous at a ∈ I iff $\lim_{x \to a} f(x) = f(a)$**
- **f is continuous iff for all a ∈ I $\lim_{x \to a} f(x) = f(a)$**
- If f is continuous at a and g is continuous at f(a), then $g \circ f$ is continuous at a
- **Intermediate value theorem: If f is continuous** and is defined at a and b **and f(a) and f(b) have opposite signs, then f(c)=0 for some c ∈ (a; b)**
- **Extreme value theorem: If f is defined for and continuous over [a; b], then $\exists$ m, M ∈ [a; b]: $\forall$x ∈ [a; b]. f(m)≤f(x)≤f(M)** — all intervals are closed

Differentiation

Differentiation

- **$f'(a)$** $= \lim_{h\to 0} = (f(a+h)-f(a))/h$ **$= \lim_{x\to a} (f(x)-f(a))/(x-a)$**
  - **f is differentiable at a iff this limit exists**
- **f is differentiable iff it is differentiable at every point in its domain**
- **f is continuous at a is necessary but not sufficient for f is differentiable at a**

  Proof that f is differentiable at a → f is continuous at a: We have that $\lim_{x\to a} (f(x)-f(a))/(x-a)$ exists, let it be c.

  Then, $\lim_{x\to a} f(x)-f(a)=c\cdot\lim_{x\to a} x-a = 0$

  So, $\lim_{x\to a} f(x)-\lim_{x\to a} f(a)=0$ and thus $\lim_{x\to a} f(x)=f(a)$ as $f(a)$ is a constant
- If f' and g' exist then:
  - $(f+g)'=f'+g'$
  - $(\lambda f)'=\lambda f'$
  - **$(f\cdot g)'=f'\cdot g+g'\cdot f$**
  - **$(g \circ f)'=(g'\circ f)\cdot f'$**
  - **$(f/g)'=(f'\cdot g-f\cdot g')/g^2$**
- **In partial differentiation (δ instead of d), all variables not on the bottom of the derivative operator are treated as constants**

Using differentiation

- a is a turning point iff there exists a closed interval I near a s.t. $\forall x \in I.\ f(x) \leq f(a)$ or $\forall x \in I.\ f(a) \leq f(x)$ iff a is a local minimum or a local maximum
- <u>Global maximum and minimum may be endpoints instead of turning points</u>
- a is a stationary point iff $f'(a)=0$ iff f is either a turning point or a point of inflection
- nth derivative test: If $f'(a)=\ldots=f^{(n-1)}(a)=0$ and $f^{(n)}$ is continuous then:
  - **n is even and $f^{(n)}(a) > 0 \Rightarrow$ a is a local minimum**
  - **n is even and $f^{(n)}(a) < 0 \Rightarrow$ a is a local maximum**
  - **n is odd and $f^{(n)}(a) \neq 0 \Rightarrow$ a is a point of inflection**
- Turning point theorem: If f is differentiable and has a turning point at a, then $f'(a)=0$
- Rolle's theorem: **If f is continuous over [a;b] and differentiable over (a;b) and $f(a)=f(b)$, then $\exists c \in (a; b)$: $f'(c)=0$**

  Proof:

  By extreme value theorem f has extreme values in [a;b]

  Case f is a constant function over (a;b): Then, $f'(c)=0$ for any choice of c

  Case f is not a constant function over (a;b): Then, extreme values must be distinct, thus $\exists c \in (a; b)$ s.t. c is a turning point and so by turning point theorem $f'(c)=0$
- Mean value theorem: **If f is continuous over [a;b] and differentiable over (a;b), then $\exists c \in (a; b)$: $f'(c)=(f(b)-f(a))/(b-a)$**

  Proof: Consider $h(x)=f(x)-(f(b)-f(a))\cdot(x-a)/(b-a)$

  Deduce that $h(a)=f(a)$ and $h(b)=f(a)(=h(a))$. Hence, by Rolle's theorem, $\exists c \in (a; b)$: $h'(c)=0$.

  Thus, as $h'(c)=f'(c)-(f(b)-f(a))/(b-a)$, $f'(c)=(f(b)-f(a))/(b-a)$

Sketching rational functions

- For $y=(ax+b)/(cx+d)$ and $y=(ax^2+bx+c)/(dx^2+ex+f)$:
  - x-intercept ⇔ numerator=0
  - y-intercept ⇔ $x=0$
  - Vertical asymptote ⇔ denominator=0
  - Horizontal asymptote ⇔ $x\to\infty$ ⇔ y is approaching a/c in first case and a/d in the second case
- To find (y-values of) stationary points set the equation equal to k (to find intersection points with y=k) then find discriminant, set that equal to 0, and solve for k
  - The set of values that y cannot take is described by discriminant < 0
- Oblique asymptotes: If $y=(ax^2+bx+c)/(ex+f)$:
  - All above rules apply except for the one for horizontal asymptotes
  - Instead, y tends towards $(ax^2+bx+c)//(ex+f)$ i.e. polynomial division but discard the remainder — this process works in all cases <u>dividing coefficients is a shortcut that only works if f=0</u>

L'hopital's rule

- Weak L'hopital's rule: **If $f(a)=g(a)=0$ and $g'(a)\neq 0$, then $\lim_{x\to a} f(x)/g(x)=f'(a)/g'(a)$**
  Proof: $\lim_{x\to a} f(x)/g(x) = \lim_{x\to a}(f(x)-f(a))/(g(x)-g(a))$
  $=(f'(a)/g'(a))\lim_{x\to a}(x-a)/(x-a)$ as limits preserve multiplication
  $= f'(a)/g'(a)$
- L'hopital's rule: **If $f(a)=g(a)=0$ and f and g are differentiable, then $\lim_{x\to a} f(x)/g(x)=\lim_{x\to a} f'(x)/g'(x)$**
- *Strong l'hopital's rule: If f and g are differentiable and $f(a)=g(a)=0$ or $f(a)=g(a)=\pm\infty$, then $\lim_{x\to a} f(x)/g(x)=\lim_{x\to a} f'(x)/g'(x)$*

Differentiation of inverse functions

- Implicit differentiation: To find dy/dx, first differentiate each term with respect to x treating y terms as functions of x using chain rule with dy/dx then rearrange for dy/dx
  - If $x^2+y^2=1$, $2x+2y\cdot dy/dx=0$ and $2x\cdot dx/dy+2y=0$
- Let $y=f(x)$, then $\mathbf{[f^{-1}(y)]'=[f'(x)]^{-1}}$ then rewrite in terms of y (e.g. by using below instead)
  Proof: By implicit differentiation, $1=f'(x)\cdot dx/dy$. So, $dx/dy=1/f'(x)$
  - *Corollary: Let $y=f(x)$, then* $\boldsymbol{[f^{-1}(y)]' \equiv [f'(f^{-1}(y))]^{-1}}$ ***— useful for differentiating inverse trig functions***
    Alternate Proof: We have that $f(f^{-1}(y)) \equiv y$
    Differentiating both sides using chain rule: $[(f^{-1}(y)]'\cdot[f'(f^{-1}(y))] = 1$

- To find d/dx(arcsin(x)):
  Let $f(x) = \sin(x)$
  Then, $f^{-1}(x) = \arcsin(x)$ and $f'(x) = \cos(x)$
  Thus, $d/dx(\arcsin(x)) = 1/\cos(\arcsin(x))$
  <u>Let $a = \arcsin(x)$</u>
  <u>Then, $\sin^2(a) + \cos^2(a) \equiv 1$ and $x = \sin(a)$</u>
  Thus, $d/dx(\arcsin(x)) = 1/\mathrm{sqrt}(1 - x^2)$

Taylor series

Taylor series

- **Taylor series of f(x) at x=a: $f(x) = \Sigma f^{(i)}(a)/n!\cdot(x-a)^i$** (if f can be differentiated any number of times)
- Taylor polynomial: $f(x) = \Sigma f^{(i)}(a)/n!\cdot(x-a)^i$ from i=0 to i=n (+ $R_n(x)$ where $R_n(x)$ is the difference between f(x) and the taylor polynomial)
  - **Taylor's theorem: If $f^{(n+1)}$ exists over (a; x)** and $f^{(n)}$ is continuous over [a; x]**, then $\exists$ c $\in$ (a;x): $R_n = f^{(n+1)}(\underline{c})/(n+1)!\cdot(x-a)^{n+1}$** *and* $\lim_{x\to a} R_n(x) = 0$
  - **For x in the radius of convergence, $\lim_{n\to\infty} R_n(x) = 0$**
- For x in the radius of convergence, $a_n = f^{(i)}(a)/n!\cdot(x-a)^i$ passes ratio test for $n \to\infty$
- Taylor series are power series!
- *Let $g(x) = \Sigma f^{(i)}(a)/n!\cdot(x-a)^i$ from i=0 to i=n. Then, g(a)=f(a) and for all N≤n $g^{(N)}(a)=f^{(N)}(a)$*
- Maclaurin series = taylor series at a=0

Integration

Integration

- Let $\{x_0, \ldots, x_n\}$ be a partition of [a; b] (a subset of [a; b] s.t. x_0=a, x_n=b, and the elements are strictly increasing)
  - Let $m_r = \min \{f(x): x \in [x_{r-1}, x_r]\}$ and $M_r = \max \{f(x): x \in [x_{r-1}, x_r]\}$
  - Let $L = \Sigma (x_r - x_{r-1}) m_r$ from r=1 to r=n and $U = \Sigma (x_r - x_{r-1}) M_r$ from r=1 to r=n
  - Then, L is the area formed by tallest rectangles that lie entirely below f and U is the area formed by shortest rectangles that lie entirely above f
  - f is integrable over [a; b] (and A is the definite integral of f between a and b) iff there exists exactly one A: $L \le A \le U$ for every partition of [a; b]
- **The following are each necessary and sufficient for f is integrable over [a;b]:**
  - **f is continuous over [a;b]**
  - **f is increasing over [a;b]**
  - **f is decreasing over [a;b]**
- First fundamental theorem of calculus: Let $f: [a; b] \mapsto \mathbb{R}$ and $F(x) = \int f(t)\, dt$ from t=a to t=x. **<u>If f is continuous at c ∈ [a;b]</u>, then F is differentiable at c and moreover F’(c)=f(c)**
- Second fundamental theorem of calculus: Let $f: [a; b] \mapsto \mathbb{R}$ and F be a function s.t. $\forall x \in [a;b]$ F’(x)=f(x). Then, $\int f(x)\, dx$ from b to a = F(b) − F(a)

(First order ordinary) Differential equations

Terminology

- Ordinary DE (ODE) = DE where all derivatives are with respect to the same variable
- Order of a DE = order of highest order derivative it contains
- In this module we only deal with first order ODEs
  - Separable iff can be written in the form $dy/dx = f(x)g(y)$
    - Then $\int 1/g(y)\, dy = \int f(x)\, dx$
  - **Homogenous iff can be written in form $dy/dx=f(y/x)$**
    - Making the **substitution $v=y/x$** gives **$\log(x) = \int 1/(f(v)-v)\, dv$** — <u>reverse substitution once evaluated</u>
      Proof: We have that $y=vx$
      Implicit differentiation with respect to x: $dy/dx = v+x \cdot dv/dx$
      $dv/dx = (dy/dx - v)/x$
      $dv/dx = (f(v) - v)(1/x)$ — separable
  - **Linear iff can be written in the form $dy/dx+P(x)y=Q(x)$**

Solving linear (the integrating factor)

- *If Q=0 for all x, then is separable (f(x)=P(x) and g(y)=1/y) and* $y=e^{\int -P(x)\,dx}$
- Let $\mathbf{I(x) = e^{\int P(x)\,dx}}$, then $I'(x)=P(x)I(X)$
- Multiplying both sides of DE by I(x) gives $I(x)y'+I'(x)y=I(x)Q(x)$
  - By the product rule, $d/dx(I(x)y) = I'(x)y + I(x)y'$. So, $d/dx(I(x)y) = I(x)Q(x)$
  - So, $\mathbf{I(x)y = \int I(x)Q(x)\,dx}$
    - **Don't need +C in I(x) but do need it here** and don't forget to divide it by I(x)
  - Thus, $y = 1/I(x)[\int I(x)Q(x)\,dx]$