IMC Cheat Sheet

Tobias Schnieders, Paul Vögele, Barbara Roos

March 31, 2025

Contents

Chapter 1

Inequalities

1.1 Basic Inequalities without a specific name

- $x \in \mathbb{R} \Rightarrow x^2 \geq 0$ with equality iff $x = 0$.
- $a, b \in \mathbb{R} \Rightarrow a^2 + b^2 \geq 2ab$ with equality iff $a = b$.

1.2 HM-GM-AM-QM Inequality[1]

Let $x_1, \ldots, x_n > 0$. Then

$$0 < \frac{n}{\frac{1}{x_1} + \cdots + \frac{1}{x_n}} \leq \sqrt[n]{x_1 \cdots x_n} \leq \frac{x_1 + \ldots + x_n}{n} \leq \sqrt{\frac{x_1^2 + \ldots x_n^2}{n}}.$$

Equality holds in each inequality iff $x_1 = \ldots = x_n$.

1.3 Weighted GM-AM Inequality

Let $x_1, \ldots, x_n > 0$ and $\theta_1, \ldots, \theta_n > 0$ such that $\theta_1 + \ldots + \theta_n = 1$. Then

$$x_1^{\theta_1} \cdot \ldots \cdot x_n^{\theta_n} \leq \theta_1 x_1 + \ldots + \theta_n x_n.$$

Equality holds iff $x_1 = \ldots = x_n$.

1.4 Jensen's inequality

Let $f\colon [a, b] \to \mathbb{R}$ be convex, $x_1, \ldots, x_n \in [a, b]$ and $\alpha_1, \ldots, \alpha_n > 0$ such that $\alpha_1 + \ldots, \alpha_n = 1$. Then

$$f\left(\sum_{i=1}^{n} \alpha_i x_i\right) \leq \sum_{i=1}^{n} \alpha_i f(x_i).$$

The inequality is reversed, if f is concave. The inequality holds for integrals instead of sums as well.

[1] Harmonic-geometric-arithmetic-quadratic mean inequality

1.5 Cauchy-Schwarz inequality

Let u and v be vectors of an inner product space. Then

$$|\langle u, v\rangle|^2 = \langle u, v\rangle \cdot \langle v, u\rangle \leq \langle u, u\rangle \cdot \langle v, v\rangle.$$

Equality holds iff u and v are linearly dependent.

In particular: Let $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in \mathbb{C}^n$. Then

$$\sum_{i=1}^{n} |x_i y_i| \leq \left(\sum_{i=1}^{n} |x_i|^2\right)^{1/2} \left(\sum_{i=1}^{n} |y_i|^2\right)^{1/2}.$$

Equality holds iff there exists a $\lambda \in \mathbb{C}$ such that $x_i = \lambda y_i$ for all $i = 1, \ldots, n$.
This is a special case of Hölder's inequality.

1.6 Hölder's inequality

Let $1 \leq p, q \leq \infty$ such that $\frac{1}{p} + \frac{1}{q} = 1$ and $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in \mathbb{C}^n$. Then

$$\sum_{i=1}^{n} |x_i y_i| \leq \left(\sum_{i=1}^{n} |x_i|^p\right)^{1/p} \left(\sum_{i=1}^{n} |y_i|^q\right)^{1/q}.$$

Here, $p = \infty$ means that the sum should be replaced by $\max(|x_1|, \ldots, |x_n|)$. Equality holds iff there exists a $\lambda \in \mathbb{C}$ such that $x_i = \lambda y_i$ for all $i = 1, \ldots, n$. The inequality holds for integrals as well.

1.7 Young's inequality

Let $a, b, p, q > 0$ with $\frac{1}{p} + \frac{1}{q} = 1$. Then

$$\frac{a^p}{p} + \frac{b^q}{q} \geq ab.$$

Equality holds iff $a^p = b^q$.

1.8 Minkowski's inequality

Let $x_1, \ldots, x_n, y_1, \ldots, y_n, m_1, \ldots, m_n > 0$ and $p > 1$. Then

$$\left(\sum_{i=1}^{n} m_i (x_i + y_i)^p\right)^{1/p} \leq \left(\sum_{i=1}^{n} m_i x_i^p\right)^{1/p} + \left(\sum_{i=1}^{n} m_i y_i^p\right)^{1/p}.$$

Equality holds iff there exists a $\lambda \in \mathbb{C}$ such that $x_i = \lambda y_i$ for all $i = 1, \ldots, n$.

1.9 Chebyshev's inequality[2]

Let $a_1 \geq \ldots \geq a_n$ and $b_1 \geq \ldots \geq b_n$. Then

$$n \sum_{i=1}^{n} a_i b_i \geq \left(\sum_{i=1}^{n} a_i\right)\left(\sum_{i=1}^{n} b_i\right) \geq n \left(\sum_{i=1}^{n} a_i b_{n+1-i}\right).$$

Equality holds on each side iff $a_1 = \ldots = a_n$ or $b_1 = \ldots = b_n$. The inequality holds for integrals as well.

[2] Also called: Chebyshev's sum inequality

1.10 Nesbitt's inequality

Let $a, b, c > 0$. Then

$$\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} \geq \frac{3}{2}.$$

Chapter 2

Combinatorics

2.1 Bijections

Two sets have the same number of elements, iff there exists a bijection between them.

2.2 The Pigeonhole Principle[1]

If n items are distributed on m boxes, with $n > m$, then at least one box contains more than one element.

Generalization:
If n items are distributed on m boxes, with $n > km$, then at least one box contains $k + 1$ elements.

2.3 Basic cardinalities

The number of permutations of a set of cardinality n is $n!$.

2.4 Inclusion-exclusion principle

This is also known as Sieve-formula. For finite sets $A_1, \ldots, A_n$ it holds that

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1} |A_1 \cap \cdots \cap A_n|.$$

[1] Also called: The Box Principle

Chapter 3

Number Theory

3.1 Bézout's identity[1]

For $a, b \in \mathbb{Z} \setminus \{0\}$ there are $x, y \in \mathbb{Z}$, such that $ax + by = \gcd(a, b)$.

Corollary: For two non-zero, coprime integers a, b, there are integers x, y such that $ax + by = 1$.

3.2 Wilson's theorem

Let $1 < p \in \mathbb{N}$. Then p is prime iff $(p-1)! \equiv -1 \pmod p$.

3.3 Fermat's little theorem

Let p be a prime number and $a \in \mathbb{Z}$. Then

$$a^p \equiv a \pmod p.$$

3.4 Euler's theorem[2]

Euler's totient function is given by

$$\varphi(n) = \#\{m \in \mathbb{N} \mid m \leq n \wedge \gcd(m, n) = 1\} = n\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right),$$

where $p_1, \dots, p_k$ are the distintct prime numbers dividing n. Let a and n be coprime positive integers. Then

$$a^{\varphi(n)} \equiv 1 \pmod n.$$

3.5 Chinese remainder theorem

Let $n_1, \dots, n_k$ be pairwise coprime positive integers and $N \coloneqq n_1 \cdots n_k$. Then

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}.$$

[1] Also called: Bézout's lemma
[2] Also called: Fermat-Euler theorem

3.6 Euclid's formula for all Pythagorean triples

All pairwise coprime triples of integers satisfying $x^2 + y^2 = z^2$ are given by

$$x = |u^2 - v^2|,\ y = 2uv,\ z = u^2 + v^2 \text{ with } \gcd(u, v) = 1,\ u \not\equiv v \pmod 2.$$

3.7 Finite Group of Units of a field

Let K be a field and S a finite subgroup of K^*. Then S is cyclic.

3.8 Fermat's theorem on sums of two squares

Let p be an odd prime number. Then there exist $a, b \in \mathbb{N}$ such that $p = a^2 + b^2$ iff $p \equiv 1 \pmod 4$.

3.9 Sophie Germain Identity

$$a^4 + 4b^4 = (a^2 + 2ab + 2b^2)(a^2 - 2ab + 2b^2).$$

3.10 Other useful facts

- $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$
  $\Rightarrow a - b \mid a^n - b^n$; if n even $a + b \mid a^n - b^n$; if n odd $a + b \mid a^n + b^n$
- Let $QS(n)$ denote the sum of the digits of n. Then $QS(n) \equiv n \mod 9$ and $QS(n) \equiv n \mod 3$.

Chapter 4

Polynomials

4.1 Fundamental theorem of algebra

Every non-constant univariate polynomial over $\mathbb{C}$ has a root in $\mathbb{C}$.

4.2 Identity theorem for polynomials

Let K be a field and $f \in K[t]$ be a polynomial of degree n with $n+1$ zeroes. Then $f = 0$.

Corollary: If two polynomials $f, g \in K[t]$ of degree n coincide in $n+1$ points, they are equal.

4.3 Interpolation

Let n be a natural number and $a_0, \dots a_n, b_0, \dots b_n$ fix complex numbers, with the a_k being all distinct. Then there is a unique polynomial P of degree $\leq n$ such that for all $0 \leq k \leq n$

$$P(a_k) = b_k.$$

If all (a_k, b_k) are rational or real, the coefficients of P are rational or real, respectively.

The polynomial P can be explicitly constructed as

$$P(x) = \sum_{k=0}^{n} b_k \cdot L_k(x),$$

where the L_k are the Lagrange-Polynomials

$$L_k(x) = \prod_{i \neq k} \frac{x - a_i}{a_k - a_i}$$

which satisfy $L_k(a_l) = \delta_{k,l}$.

4.4 Luca's theorem

The zeros of the derivative $P'(z)$ of a polynomial $P \in \mathbb{C}[z]$ lie in the convex hull of the zeros of $P(z)$.

4.5 Reciprocal polynomials

We call a polynomial $f = a_n x^n + \ldots + a_1 x + a_0 \neq 0$ *reciprocal*, if $a_i = a_{n-i}$ for $i = 0, \ldots, n$.
A reciprocal polynomial f of degree $2n$ can be written in the form $f = x^n g\left(x + \frac{1}{x}\right)$, where g is a polynomial of degree n.

4.6 Fundamental theorem of symmetric polynomials

Let R be a commutative unital ring. For every symmetric polynomial $f \in R[x_1, \ldots, x_n]$ exists exactly one polynomial $g \in R[y_1, \ldots, y_n]$, such that

$$f(x_1, \ldots, x_n) = g(e_1(x_1, \ldots, x_n), \ldots, e_n(x_1, \ldots, x_n)).$$

Here, e_k denotes the k-th elementary symmetric polynomial

$$e_k(x_1, \ldots x_n) = \sum_{i_1 < \cdots < i_k} x_{i_1} \cdots x_{i_k}.$$

4.7 Vietà

Let $P(x) = a_n x^n + \ldots a_1 x + a_0$ with $a_n \neq 0$. Let $\alpha_1, \ldots \alpha_n$ be the roots of P (counted with multiplicity). Then

$$e_k(\alpha_1, \ldots, \alpha_n) = (-1)^k \frac{a_{n-k}}{a_n}, \quad \text{for } 1 \leq k \leq n.$$

4.8 Eisenstein

Let $P(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$. If there is a prime number p such that $p \not| a_n$, $p | a_0, \ldots a_{n-1}$ and $p^2 \not| a_0$, $P(x)$ is irreducible over $\mathbb{Z}[x]$.

Chapter 5

Linear Algebra and Matrices

5.1 The Adjugate

Let R be a commutative unital ring and $A \in \mathrm{Mat}_n(R)$. Then

$$AA^{\#} = \det(A)\mathbb{1}_n.$$

Corollary:

$$A \text{ invertible} \Leftrightarrow \det(A) \text{ invertible}.$$

5.2 Rank-1 Matrices

A matrix $A \in \mathrm{Mat}(m \times n, K)$ has rank 1 if and only if it can be written as $A = vw^t$ for vectors $v \in K^m$ and $w \in K^n$.

5.3 Cyclicity of the trace

The trace is cyclic, i.e. $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ for two square matrices A and B.

5.4 Spectral theorem

Let $K \in \{\mathbb{R}, \mathbb{C}\}$ and $A \in \mathrm{Mat}_n K$ be a normal matrix with eigenvalues in K. Then A is unitary diagonalisable, i.e. there is a unitary matrix $U \in \mathrm{Mat}_n K$ such that U^*AU is diagonal.

Corollary: A symmetric matrix $A \in \mathrm{Mat}_n\mathbb{R}$ is orthogonally diagonalisable.

5.5 Cayley-Hamilton theorem

Any $n \times n$ matrix A satisfies its characteristic equation, which means that if $P_A(\lambda) = \det(\lambda_n - A)$, then $P_A(A) = 0$. Equivalently, the minimal polynomial of A divides the characteristic polynomial of A.

5.6 Perron-Frobenius

Any square matrix with positive entries has a unique eigenvector with positive entries (up to mult. by a positive scalar), and the corresponding eigenvalue has multiplicity one and is strictly greater than the absolute value of any other eigenvalue.

Chapter 6

Calculus

6.1 Weierstrass extreme value theorem

A continuous function on a compact set attains its maximum and minimum.

6.2 Intermediate value theorem

Let $f\colon [a,b] \to \mathbb{R}$ be a continuous function and $\min(f(a), f(b)) < c < \max(f(a), f(b))$.
Then there is a point $\xi \in (a,b)$ such that $f(\xi) = c$.

Equivalently:
Let $f\colon [a,b] \to \mathbb{R}$ be a continuous function and $f(a)f(b) < 0$. Then f has a zero in (a,b).

6.3 Mean value theorem

Let $f, g\colon [a,b] \to \mathbb{R}$ be continuous and differentiable on (a,b). Then there is a point $\xi \in (a,b)$ such that

$$(f(b) - f(a))g'(\xi) = (g(b) - g(a))f'(\xi).$$

Choosing $g(x) = x$, we obtain the Lagrange theorem that there is a point $\xi \in (a,b)$ such that

$$f'(\xi) = \frac{f(b) - f(a)}{b - a}.$$

6.4 Mean value theorem for integrals

Let $f\colon [a,b] \to \mathbb{R}$ be continuous. Then there existst a $\xi \in (a,b)$ such that

$$(b - a)f(\xi) = \int_a^b f(x)\mathrm{d}x.$$

6.5 Tangent half-angle substitution

The substitution $t := \tan\left(\frac{x}{2}\right)$ can be used to solve several integrals. In particular

$$\int f\left(\sin(x), \cos(x)\right) dx = \int f\left(\frac{2t}{1+t^2}, \frac{1-t^2}{1+t^2}\right) \frac{2}{1+t^2} dt.$$

Chapter 7

Functional equations

Functional equations are about finding functions satisfying certain equations. Often it is useful to plug in values and play around. If there are some special assumptions on the functions (e.g. continuity or differentiability) it probably is helpful to use these properties.

7.1 Cauchy's functional equation

Which functions $f : \mathbb{R} \to \mathbb{R}$ satisfy

$$f(x + y) = f(x) + f(y)?$$

If we assume that f should be continuous in at least one point, the solutions to this functional equation are given by $f(x) = cx$, where $c \in \mathbb{R}$. If we do not assume continuity, there are many solutions (Putnam and Beyond, Chapter 3.4.1).

Chapter 8

Algebra

8.1 Lagrange theorem

Let G be a group and H a subgroup of G. Then

$$|G| = |G/H| \cdot |H|.$$

In a finite group G thus $|H|$, $|G/H|$ and the order of any element $g \in G$ divide $|G|$. If $|G|$ is prime, the group G is cyclic and only has the subgroups 1 and G.

8.2 Subgroups of additive real numbers

A nontrivial subgroup of the additive group of real numbers is either cyclic or it is dense in the set of real numbers. (see Putnam and beyond, Section 2.4.3)

8.3 Sylow's theorems

Let p be prime. A finite group of order p^k for some $k \geq 1$ is called *p-group*. Let G be a finite group and p a prime divisor of $|G|$. Write $|G| = p^k m$ for $k, m \geq 1$ with $p \not| m$. Every subgroup of G of order p^k is called Sylow p-subgroup of G. The theorems state

(i) There exists a Sylow p-subgroup of G.

(ii) Every p-subgroup of G is contained in a Sylow p-subgroup of G.

(iii) All Sylow p-subgroups are conjugate to each other.

(iv) The number of Sylow p-subgroups of G is $\equiv 1 \mod p$ and a divisor of m.

It follows as a corollary, that G has an element of order p.

8.4 Symmetric group

The group S_n of all permutations of $\{1, \ldots, n\}$ is called the symmetric group of degree n. Its order is $|S_n| = n!$. Every permutation is a product of disjoint cycles. The group S_n is generated by transpositions.

Cayley theorem Every finite group is isomorphic to a subgroup of some S_n.

8.5 Jacobson's theorem.

If R is a ring and for every $x \in R$ there exists an integer $n(x) > 1$ such that $x^{n(x)} = x$, then the ring is commutative.

Chapter 9

Sequences and Series

9.1 Binomial series

Let $\alpha, x \in \mathbb{C}$ such that $|x| < 1$ or $\alpha \in \mathbb{N}$. Then:

$$(1+x)^\alpha = 1 + \alpha x + \frac{\alpha(\alpha-1)}{2!}x^2 + \frac{\alpha(\alpha-1)(\alpha-2)}{3!}x^3 + \frac{\alpha(\alpha-1)(\alpha-2)(\alpha-3)}{4!}x^4 + \dots$$

9.2 Generating function[1]

The generating function of a given sequence (a_n) is

$$f(x) := \sum_{n=0}^{\infty} a_n x^n.$$

Finding an explicit formula for a recursively given sequence can often be reduced to finding and solving functional equations of the corresponding generating function.

To avoid issues like certain manipulations being prohibited by the rules of calculus, e.g. caring about convergence, f will at first glance not be seen as a function. Instead, f is seen as a formal power series. However, it is advisable to try certain manipulations known from calculus. Many of those do still work, as the formal power series form a complete local ring and as the formal derivation works alike for formal power series. Caring about the rules of calculus can often be done retroactively, if necessary.

9.3 Exponential generating function

The exponential generating function of a given sequence (a_n) is

$$f(x) := \sum_{n=0}^{\infty} a_n \frac{x^n}{n!}.$$

Finding an explicit formula for a recursively given sequence can sometimes be reduced to finding and solving functional equations of the corresponding exponential generating function.
In doing so, the theory of exponential generating functions can be applied similar to the theory of generating functions.

[1] Also called: Ordinary generating function

Chapter 10

Geometry

10.1 Triangle inequality

Let $a, b, c > 0$. Then the following statements are equivalent:

(a) a, b, c are the sides of a non-degenerate triangle.

(b) $a + b > c$ and all permutations of this inequality also hold.

(c) There are $x, y, z > 0$ such that $a = y+z,\ b = x+z,\ c = x+y$ (Also called geometric substitution)

10.2 Comparing sides and angles of a triangle

Consider a triangle with sides a, b, c and angles α, β, γ, respectively. Then

$$a > b \Leftrightarrow \alpha > \beta.$$

All permutations of this equivalence hold as well.

10.3 Inscribed angle theorem

An angle inscribed in a circle is half of the central angle subtending the same arc.

Corollary: Let A, B be points in the plane and $0 < \alpha < \pi$. The set of points P such that $\angle APB = \alpha$ is an arc of a circle, bounded by A and B.

10.4 Ptolemy's theorem

For any four points A, B, C, D in the plane, the following inequality holds:

$$AC \cdot BD \leq AB \cdot CD + AD \cdot BC.$$

Equality holds iff $ABCD$ is a cyclic quadrilateral[1] or A, B, C, D are collinear with exactly one of B, D between A, C.

[1] Also called: Chordal quadrilateral

10.5 Parallelogram inequality

For any four points $A, B, C, D \in \mathbb{R}^n$ we have

$$AB^2 + BC^2 + CD^2 + DA^2 \geq AC^2 + BD^2$$

with equality[2] iff $ABCD$ is a parallelogram with diagonals AC and BD.

10.6 Heron's formula

Consider a triangle with sides a, b, c. Then the area of the triangle is given by

$$\sqrt{s(s-a)(s-b)(s-c)}.$$

Here, $s := \frac{a+b+c}{2}$ denotes the semiperimeter of the triangle.

10.7 Law of sines

Consider a triangle with sides a, b, c, angles α, β, γ, respectively, and circumcircle radius R. Then

$$\frac{a}{\sin(\alpha)} = \frac{b}{\sin(\beta)} = \frac{c}{\sin(\gamma)} = 2R.$$

10.8 Law of cosines

Consider a triangle with sides a, b, c and angles α, β, γ, respectively. Then

$$c^2 = a^2 + b^2 - 2ab\cos(\gamma).$$

10.9 Weitzenböck's inequality

Consider a triangle with sides a, b, c and area A. Then

$$a^2 + b^2 + c^2 \geq 4\sqrt{3} \cdot A.$$

10.10 Erdös-Mordell inequality

Consider the triangle ABC. Let P be a point inside the triangle. Let PF_a, PF_b and PF_c be the perpendiculars from P to each side of the triangle. Then

$$PA + PB + PC \geq 2\left(PF_a + PF_b + PF_c\right).$$

[2] If $ABCD$ is a parallelogram, this equation is called Parallelogram identity