Algebra

IMC 2022 Training

Robin Visser
Mathematics Institute
University of Warwick

1 July 2022

Overview

1. Linear Algebra
2. Polynomials
3. Inequalities
4. Group Theory
5. Number Theory

Linear Algebra

- Let V be a vector space over a field F.

Linear Algebra

- Let V be a vector space over a field F.

Linear Independence

A set of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is **linearly independent** if the only scalars $\alpha_1, \ldots, \alpha_n$ which satisfy

$$\alpha_1 \mathbf{v}_1 + \cdots + \alpha_n \mathbf{v}_n = \mathbf{0}$$

are $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$.

Linear Algebra

- Let V be a vector space over a field F.

Linear Independence

A set of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is **linearly independent** if the only scalars $\alpha_1, \ldots, \alpha_n$ which satisfy

$$\alpha_1 \mathbf{v}_1 + \cdots + \alpha_n \mathbf{v}_n = \mathbf{0}$$

are $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$.

Span

A set of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ **spans** V if, for all vectors $\mathbf{w} \in V$, there exist scalars $\beta_1, \ldots, \beta_n$ such that

$$\beta_1 \mathbf{v}_1 + \cdots + \beta_n \mathbf{v}_n = \mathbf{w}$$

Linear Algebra

- Let V be a vector space over a field F.

Linear Independence

A set of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is **linearly independent** if the only scalars $\alpha_1, \ldots, \alpha_n$ which satisfy

$$\alpha_1 \mathbf{v}_1 + \cdots + \alpha_n \mathbf{v}_n = \mathbf{0}$$

are $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$.

Span

A set of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ **spans** V if, for all vectors $\mathbf{w} \in V$, there exist scalars $\beta_1, \ldots, \beta_n$ such that

$$\beta_1 \mathbf{v}_1 + \cdots + \beta_n \mathbf{v}_n = \mathbf{w}$$

Basis

A set of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is a **basis** for V if it is linearly independent and spans V.

Linear Algebra

Useful facts:

- Every vector space has a basis.
- All bases of V have the same cardinality. This is the **dimension** of V.
- Any linearly independent set can be extended to a basis.
- Any spanning set can be reduced to a basis.
- Any set of non-zero pairwise orthogonal vectors is a linearly independent set.
- If V is a vector space of dimension n, then the following are equivalent for a set of n vectors $S = \{v_1, \ldots, v_n\}$:
  - S is linearly independent
  - S spans V
  - S is a basis

Example

Example

Let V be a 10-dimensional real vector space and U_1 and U_2 two linear subspaces such that $U_1 \subseteq U_2$, $\dim_{\mathbb{R}} U_1 = 3$ and $\dim_{\mathbb{R}} U_2 = 6$. Let $\mathcal{E}$ be the set of all linear maps $T : V \to V$ which have U_1 and U_2 as invariant subspaces (i.e. $T(U_1) \subseteq U_1$ and $T(U_2) \subseteq U_2$). Calculate the dimension of $\mathcal{E}$ as a real vector space.

Example

Example

Let V be a 10-dimensional real vector space and U_1 and U_2 two linear subspaces such that $U_1 \subseteq U_2$, $\dim_{\mathbb{R}} U_1 = 3$ and $\dim_{\mathbb{R}} U_2 = 6$. Let $\mathcal{E}$ be the set of all linear maps $T : V \to V$ which have U_1 and U_2 as invariant subspaces (i.e. $T(U_1) \subseteq U_1$ and $T(U_2) \subseteq U_2$). Calculate the dimension of $\mathcal{E}$ as a real vector space.

Example

Let k be a positive integer. Find the smallest positive integer n for which there exist k nonzero vectors $v_1, \ldots, v_k$ in $\mathbb{R}^n$ such that for every pair i, j of indices with $|i - j| > 1$ the vectors v_i and v_j are orthogonal.

Example

Example

Let V be a 10-dimensional real vector space and U_1 and U_2 two linear subspaces such that $U_1 \subseteq U_2$, $\dim_{\mathbb{R}} U_1 = 3$ and $\dim_{\mathbb{R}} U_2 = 6$. Let $\mathcal{E}$ be the set of all linear maps $T : V \to V$ which have U_1 and U_2 as invariant subspaces (i.e. $T(U_1) \subseteq U_1$ and $T(U_2) \subseteq U_2$). Calculate the dimension of $\mathcal{E}$ as a real vector space.

Example

Let k be a positive integer. Find the smallest positive integer n for which there exist k nonzero vectors $v_1, \ldots, v_k$ in $\mathbb{R}^n$ such that for every pair i, j of indices with $|i - j| > 1$ the vectors v_i and v_j are orthogonal.

Hint: Consider the vectors $v_1, v_3, v_5, \ldots$.

Matrices

Matrices

An $m \times n$ **matrix** is a rectangular array of numbers

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

Matrices

Matrices

An $m \times n$ **matrix** is a rectangular array of numbers

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

- **Determinant:**

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

- **Trace:**

$$\operatorname{tr}(A) = a_{11} + a_{22} + \cdots + a_{nn}$$

- **Eigenvalues:**

$$\lambda_i \text{ where } Av = \lambda_i v \text{ for some non-zero vector } v$$

Determinants

Row operations:

- Multiply row/column by c multiples the determinant by c.
- Swapping two rows/columns multiples determinant by -1.
- Adding scalar multiple of one row to another row does not change determinant.

Determinants

Row operations:

- Multiply row/column by c multiples the determinant by c.
- Swapping two rows/columns multiples determinant by -1.
- Adding scalar multiple of one row to another row does not change determinant.

Useful properties:

- Homogenuity: $\det(cA) = c^n \det(A)$
- Multiplicativity: $\det(AB) = \det(A)\det(B)$
- A is invertible $\iff \det(A) \neq 0$.
- Transpositions: $\det(A^T) = \det(A)$
- Product of eigenvalues: $\det(A) = \lambda_1 \lambda_2 \cdots \lambda_n$ (counted with multiplicity)
- If A is triangular, then $\det(A) = a_{11} a_{22} \cdots a_{nn}$.
- Cofactor expansion: $\det(A) = (-1)^{i+1} a_{i1} M_{i1} + (-1)^{i+2} a_{i2} M_{i2} + \cdots + (-1)^{i+n} a_{in} M_{in}$

Determinants

Example

(a) Show that for any $m \in \mathbb{N}$ there exists a real $m \times m$ matrix A such that $A^3 = A + I$, where I is the $m \times m$ identity matrix.

(b) Show that $\det A > 0$ for every real $m \times m$ matrix satisfying $A^3 = A + I$.

Determinants

Example

(a) Show that for any $m \in \mathbb{N}$ there exists a real $m \times m$ matrix A such that $A^3 = A + I$, where I is the $m \times m$ identity matrix.

(b) Show that $\det A > 0$ for every real $m \times m$ matrix satisfying $A^3 = A + I$.

Example

For any integer $n \geq 2$ and two $n \times n$ matrices with real entries A, B that satisfy the equation $A^{-1} + B^{-1} = (A + B)^{-1}$ prove that $\det(A) = \det(B)$.

Determinants

Example

(a) Show that for any $m \in \mathbb{N}$ there exists a real $m \times m$ matrix A such that $A^3 = A + I$, where I is the $m \times m$ identity matrix.

(b) Show that $\det A > 0$ for every real $m \times m$ matrix satisfying $A^3 = A + I$.

Example

For any integer $n \geq 2$ and two $n \times n$ matrices with real entries A, B that satisfy the equation $A^{-1} + B^{-1} = (A + B)^{-1}$ prove that $\det(A) = \det(B)$.

Example

Let A be a real $n \times n$ matrix and suppose that for every positive integer m there exists a real symmetric matrix B such that $2021B = A^m + B^2$. Prove that $|\det A| \leq 1$.

Trace

Useful properties:

- Linearity: $\mathrm{tr}(A + b) = \mathrm{tr}(A) + \mathrm{tr}(B)$ and $\mathrm{tr}(cA) = c\mathrm{tr}(A)$
- Cyclic: $\mathrm{tr}(AB) = \mathrm{tr}(BA)$
- Transpositions: $\mathrm{tr}(A) = \mathrm{tr}(A^T)$
- Sum of eigenvalues: $\mathrm{tr}(A) = \lambda_1 + \lambda_2 + \cdots + \lambda_n$ (counted with multiplicity)
- (More generally): $\mathrm{tr}(A^k) = \lambda_1^k + \lambda_2^k + \cdots + \lambda_n^k$ (counted with multiplicity)

Trace

Useful properties:

- Linearity: $\mathrm{tr}(A+b) = \mathrm{tr}(A) + \mathrm{tr}(B)$ and $\mathrm{tr}(cA) = c\mathrm{tr}(A)$
- Cyclic: $\mathrm{tr}(AB) = \mathrm{tr}(BA)$
- Transpositions: $\mathrm{tr}(A) = \mathrm{tr}(A^T)$
- Sum of eigenvalues: $\mathrm{tr}(A) = \lambda_1 + \lambda_2 + \cdots + \lambda_n$ (counted with multiplicity)
- (More generally): $\mathrm{tr}(A^k) = \lambda_1^k + \lambda_2^k + \cdots + \lambda_n^k$ (counted with multiplicity)

Example

Determine all pairs (a, b) of real numbers for which there exists a unique symmetric 2×2 matrix M with real entries satisfying $\mathrm{trace}(M) = a$ and $\det(M) = b$.

Trace

Useful properties:

- Linearity: $\mathrm{tr}(A+b) = \mathrm{tr}(A) + \mathrm{tr}(B)$ and $\mathrm{tr}(cA) = c\mathrm{tr}(A)$
- Cyclic: $\mathrm{tr}(AB) = \mathrm{tr}(BA)$
- Transpositions: $\mathrm{tr}(A) = \mathrm{tr}(A^T)$
- Sum of eigenvalues: $\mathrm{tr}(A) = \lambda_1 + \lambda_2 + \cdots + \lambda_n$ (counted with multiplicity)
- (More generally): $\mathrm{tr}(A^k) = \lambda_1^k + \lambda_2^k + \cdots + \lambda_n^k$ (counted with multiplicity)

Example

Determine all pairs (a, b) of real numbers for which there exists a unique symmetric 2×2 matrix M with real entries satisfying $\mathrm{trace}(M) = a$ and $\det(M) = b$.

Example

Does there exist a real 3×3 matrix A such that $\mathrm{tr}(A) = 0$ and $A^2 + A^t = I$?

Rank

Rank

Let A be an $m \times n$ matrix. The (column) **rank** of A is the maximal number of linearly independent columns of A.

Rank

Rank

Let A be an $m \times n$ matrix. The (column) **rank** of A is the maximal number of linearly independent columns of A.

- Column rank $=$ row rank
- An square $n \times n$ matrix A is invertible $\iff$ $\text{rank}(A) = n$.
- **Decomposition:** $rank(A)$ is the smallest k such that there exists an $m \times k$ matrix C, and an $k \times n$ matrix R such that $A = CR$.
- **Largest minor:** $rank(A)$ is the largest k such that there is a $k \times k$ submatrix of A with non-zero determinant.
- Number of non-zero eigenvalues of A is at most $rank(A)$.
- Row operations do not change rank.
- **Sub-additivity:** $rank(A + B) \leq rank(A) + rank(B)$.

Examples

Example

Let X be a nonsingular matrix with columns $X_1, X_2, \ldots, X_n$. Let Y be a matrix with columns $X_2, X_3, \ldots, X_n, 0$. Show that the matrices $A = YX^{-1}$ and $B = X^{-1}Y$ have rank $n-1$ and have only 0's for eigenvalues.

Examples

Example

Let X be a nonsingular matrix with columns $X_1, X_2, \ldots, X_n$. Let Y be a matrix with columns $X_2, X_3, \ldots, X_n, 0$. Show that the matrices $A = YX^{-1}$ and $B = X^{-1}Y$ have rank $n-1$ and have only 0's for eigenvalues.

Example

Let A be the $n \times n$ matrix, whose (i,j)-th entry is $i+j$ for all $i,j = 1, 2, \ldots, n$. What is the rank of A?

Examples

Example

Let X be a nonsingular matrix with columns $X_1, X_2, \ldots, X_n$. Let Y be a matrix with columns $X_2, X_3, \ldots, X_n, 0$. Show that the matrices $A = YX^{-1}$ and $B = X^{-1}Y$ have rank $n-1$ and have only 0's for eigenvalues.

Example

Let A be the $n \times n$ matrix, whose (i,j)-th entry is $i+j$ for all $i,j = 1,2,\ldots,n$. What is the rank of A?

Example

Let n be a fixed positive integer. Determine the smallest possible rank of an $n \times n$ matrix that has zeros along the main diagonal and strictly positive real numbers off the main diagonal.

Cayley-Hamilton Theorem

Theorem (Cayley-Hamilton)

Let A be an $n \times n$ matrix with characteristic polynomial $p(x) := det(A - xI)$. Then $p(A) = 0$.

Cayley-Hamilton Theorem

Theorem (Cayley-Hamilton)

Let A be an $n \times n$ matrix with characteristic polynomial $p(x) := \mathit{det}(A - xI)$. Then $p(A) = 0$.

Example

Determine all rational numbers a for which the matrix

$$A = \begin{pmatrix} a & -a & -1 & 0 \\ a & -a & 0 & -1 \\ 1 & 0 & a & -a \\ 0 & 1 & a & -a \end{pmatrix}$$

is the square of a matrix with all rational entries.

Cayley-Hamilton Theorem

Theorem (Cayley-Hamilton)

Let A be an $n \times n$ matrix with characteristic polynomial $p(x) := det(A - xI)$. Then $p(A) = 0$.

Example

Determine all rational numbers a for which the matrix

$$A = \begin{pmatrix} a & -a & -1 & 0 \\ a & -a & 0 & -1 \\ 1 & 0 & a & -a \\ 0 & 1 & a & -a \end{pmatrix}$$

is the square of a matrix with all rational entries.

Hint: Suppose that $A = B^2$. What can be the minimal polynomial of B?

Polynomials

Some useful facts:

Theorem (Factor theorem)

A polynomial $f(x)$ is divisible by $x - a$ if and only if $f(a) = 0$.

Theorem (Rational root theorem)

Let $f(x) = a_n x^n + \cdots + a_0$ be a polynomial with integer coefficients. If $\frac{p}{q}$ is a rational root of f, with p, q coprime, then $p \mid a_0$ and $q \mid a_n$.

Theorem (Fundamental theorem of algebra)

Every nonconstant polynomial with complex coefficients has a complex root.

Examples

Example

Let $f : \mathbb{R} \to \mathbb{R}$ be a function such that $(f(x))^n$ is a polynomial for every $n = 2, 3, \ldots$. Does it follow that f is a polynomial?

Examples

Example

Let $f : \mathbb{R} \to \mathbb{R}$ be a function such that $(f(x))^n$ is a polynomial for every $n = 2, 3, \ldots$. Does it follow that f is a polynomial?

Example

Let n, k be positive integers and suppose that the polynomial $x^{2k} - x^k + 1$ divides $x^{2n} + x^n + 1$. Prove that $x^{2k} + x^k + 1$ divides $x^{2n} + x^n + 1$.

Examples

Example

Let $f : \mathbb{R} \to \mathbb{R}$ be a function such that $(f(x))^n$ is a polynomial for every $n = 2, 3, \ldots$. Does it follow that f is a polynomial?

Example

Let n, k be positive integers and suppose that the polynomial $x^{2k} - x^k + 1$ divides $x^{2n} + x^n + 1$. Prove that $x^{2k} + x^k + 1$ divides $x^{2n} + x^n + 1$.

Example

Let a be a rational number and let n be a positive integer. Prove that the polynomial $X^{2^n}(X + a)^{2^n} + 1$ is irreducible in the ring $\mathbb{Q}[X]$ of polynomials with rational coefficients.

Symmetric polynomials

Symmetric polynomial

A **symmetric polynomial** in n variables is a polynomial $p(x_1, \ldots, x_n)$ that does not change on permuting the variables.

Symmetric polynomials

Symmetric polynomial

A **symmetric polynomial** in n variables is a polynomial $p(x_1, \ldots, x_n)$ that does not change on permuting the variables.

Elementary symmetric polynomial

Let n be a positive integer and k a non-negative integer. The k-th **elementary symmetric polynomial** $e_k(x_1, x_2, \ldots, x_n)$ is

$$e_k(x_1, x_2, \ldots, x_n) := \sum_{1 \leq j_1 < j_2 < \cdots < j_k \leq n} x_{j_1} x_{j_2} \cdots x_{j_k}$$

i.e. the sum of all distinct products of k distinct variables.

Symmetric polynomials

Theorem (Fundamental theorem of symmetric polynomials)

Every symmetric polynomial $p(x_1, \ldots, x_n)$ can be expressed as a polynomial in the elementary symmetric polynomials $e_1, \ldots, e_n$.

Symmetric polynomials

Theorem (Fundamental theorem of symmetric polynomials)

Every symmetric polynomial $p(x_1, \ldots, x_n)$ can be expressed as a polynomial in the elementary symmetric polynomials $e_1, \ldots, e_n$.

Theorem (Vieta's formulae)

Let $p(x) = x^n + c_1 x^{n-1} + \cdots + c_n$ be a complex polynomial which factorises over $\mathbb{C}$ as

$$p(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

Then $c_k = (-1)^k e_k(\alpha_1, \ldots, \alpha_n)$ for $k = 1, 2, \ldots, n$.

Symmetric polynomials

Theorem (Fundamental theorem of symmetric polynomials)

Every symmetric polynomial $p(x_1, \ldots, x_n)$ can be expressed as a polynomial in the elementary symmetric polynomials $e_1, \ldots, e_n$.

Theorem (Vieta's formulae)

Let $p(x) = x^n + c_1 x^{n-1} + \cdots + c_n$ be a complex polynomial which factorises over $\mathbb{C}$ as

$$p(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

Then $c_k = (-1)^k e_k(\alpha_1, \ldots, \alpha_n)$ for $k = 1, 2, \ldots, n$.

Theorem (Newton-Girard)

Let n be a positive integer and let $s_k = x_1^k + \cdots + x_n^k$. Then

$$k e_k = s_1 e_{k-1} - s_2 e_{k-2} + \cdots + (-1)^k s_{k-1} e_1 + (-1)^{k-1} s_k$$

Example

Example

Find all prime numbers p for which there exists a unique $a \in \{1, 2, \ldots, p\}$ such that $a^3 - 3a + 1$ is divisible by p.

Example

Example

Find all prime numbers p for which there exists a unique $a \in \{1, 2, \ldots, p\}$ such that $a^3 - 3a + 1$ is divisible by p.

Hint: Compute the roots of $f(x) = x^3 - 3x + 1$ over $\mathbb{C}$ and find a connection between them. Or, compute the discriminant of $f(x)$ (note $\mathrm{Disc}(x^3 + px + q) = -4p^3 - 27q^2$).

Example

Example

Find all prime numbers p for which there exists a unique $a \in \{1, 2, \ldots, p\}$ such that $a^3 - 3a + 1$ is divisible by p.

Hint: Compute the roots of $f(x) = x^3 - 3x + 1$ over $\mathbb{C}$ and find a connection between them. Or, compute the discriminant of $f(x)$ (note $\mathrm{Disc}(x^3 + px + q) = -4p^3 - 27q^2$).

Example

Does there exist a sequence (a_n) of complex numbers such that for every positive integer p we have that $\sum_{n=1}^{\infty} a_n^p$ converges if and only if p is not a prime?

Example

Example

Find all prime numbers p for which there exists a unique $a \in \{1, 2, \ldots, p\}$ such that $a^3 - 3a + 1$ is divisible by p.

Hint: Compute the roots of $f(x) = x^3 - 3x + 1$ over $\mathbb{C}$ and find a connection between them. Or, compute the discriminant of $f(x)$ (note $\mathrm{Disc}(x^3 + px + q) = -4p^3 - 27q^2$).

Example

Does there exist a sequence (a_n) of complex numbers such that for every positive integer p we have that $\sum_{n=1}^{\infty} a_n^p$ converges if and only if p is not a prime?

Hint: Let $\mathbb{N} = C \cup D$ be an arbitrary decomposition of $\mathbb{N}$ into two disjoint sets. Show that for any positive integer k, there exist complex numbers $z_1, \ldots, z_k$ with the property

$$\sum_{j=1}^{k} z_j^p = \begin{cases} 0 & \text{if } p \in C \cap [1, k] \\ 1 & \text{if } p \in D \cap [1, k] \end{cases}$$

Inequalities

Theorem (Arithmetic Mean - Geometric Mean)

Let $x_1, x_2, \ldots, x_n$ be a set of nonnegative real numbers. Then

$$\frac{x_1 + x_2 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 x_2 \cdots x_n}$$

and equality holds if and only if $x_1 = x_2 = \cdots = x_n$.

Inequalities

Theorem (Arithmetic Mean - Geometric Mean)

Let $x_1, x_2, \ldots, x_n$ be a set of nonnegative real numbers. Then

$$\frac{x_1 + x_2 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 x_2 \cdots x_n}$$

and equality holds if and only if $x_1 = x_2 = \cdots = x_n$.

Theorem (QM-AM-GM-HM)

More generally

$$\sqrt{\frac{x_1^2 + \cdots + x_n^2}{n}} \geq \frac{x_1 + x_2 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 x_2 \cdots x_n} \geq \frac{n}{1/x_1 + \cdots + 1/x_n}$$

Each inequality becomes equality if and only if $x_1 = x_2 = \cdots = x_n$.

Examples

Example

Let $(a_n)_{n=1}^{\infty}$ and $(b_n)_{n=1}^{\infty}$ be two sequences of positive numbers. Show that the following statements are equivalent:

1. There is a seq $(c_n)_{n=1}^{\infty}$ of positive reals such that $\sum_{n=1}^{\infty} \frac{a_n}{c_n}$ and $\sum_{n=1}^{\infty} \frac{c_n}{b_n}$ both converge;
2. $\sum_{n=1}^{\infty} \sqrt{\frac{a_n}{b_n}}$ converges.

Examples

Example

Let $(a_n)_{n=1}^{\infty}$ and $(b_n)_{n=1}^{\infty}$ be two sequences of positive numbers. Show that the following statements are equivalent:

1. There is a seq $(c_n)_{n=1}^{\infty}$ of positive reals such that $\sum_{n=1}^{\infty} \frac{a_n}{c_n}$ and $\sum_{n=1}^{\infty} \frac{c_n}{b_n}$ both converge;
2. $\sum_{n=1}^{\infty} \sqrt{\frac{a_n}{b_n}}$ converges.

Example

Find all polynomials $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ $(a_n \neq 0)$ satisfying the following two conditions:

(i) $(a_0, a_1, \ldots, a_n)$ is a permutation of the numbers $(0, 1, \ldots, n)$; and

(ii) all roots of $P(x)$ are rational numbers.

Inequalities

Theorem (Cauchy-Schwarz inequality)

For any real numbers $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$, we have

$$(a_1 b_1 + a_2 b_2 + \cdots + a_n b_n)^2 \leq (a_1^2 + \cdots + a_n^2)(b_1^2 + \cdots + b_n^2)$$

(i.e. as vectors: $|\mathbf{a} \cdot \mathbf{b}| \leq ||\mathbf{a}||\,||\mathbf{b}||$, with equality if and only if $\mathbf{a}$ and $\mathbf{b}$ are linearly dependent)

Inequalities

Theorem (Cauchy-Schwarz inequality)

For any real numbers $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$, we have

$$(a_1 b_1 + a_2 b_2 + \cdots + a_n b_n)^2 \leq (a_1^2 + \cdots + a_n^2)(b_1^2 + \cdots + b_n^2)$$

(i.e. as vectors: $|\mathbf{a} \cdot \mathbf{b}| \leq ||\mathbf{a}||\,||\mathbf{b}||$, with equality if and only if $\mathbf{a}$ and $\mathbf{b}$ are linearly dependent)

Theorem (Cauchy-Schwarz "in Engel form")

For any real $a_1, \ldots, a_n$ and positive real $b_1, \ldots, b_n$, we have

$$\frac{a_1^2}{b_1} + \frac{a_2^2}{b_2} + \cdots + \frac{a_n^2}{b_n} \geq \frac{(a_1 + a_2 + \cdots + a_n)^2}{b_1 + \cdots + b_n}$$

Examples

Example

Let n be a positive integer. Also let $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ be real numbers such that $a_i + b_i > 0$ for $i = 1, 2, \ldots, n$. Prove that

$$\sum_{i=1}^{n} \frac{a_i b_i - b_i^2}{a_i + b_i} \leq \frac{\sum_{i=1}^{n} a_i \cdot \sum_{i=1}^{n} b_i - \left(\sum_{i=1}^{n} b_i\right)^2}{\sum_{i=1}^{n}(a_i + b_i)}$$

Examples

Example

Let n be a positive integer. Also let $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ be real numbers such that $a_i + b_i > 0$ for $i = 1, 2, \ldots, n$. Prove that

$$\sum_{i=1}^{n} \frac{a_i b_i - b_i^2}{a_i + b_i} \leq \frac{\sum_{i=1}^{n} a_i \cdot \sum_{i=1}^{n} b_i - \left(\sum_{i=1}^{n} b_i\right)^2}{\sum_{i=1}^{n}(a_i + b_i)}$$

Example

Suppose that a, b, c are real numbers in the interval $[1, 1]$ such that $1 + 2abc \geq a^2 + b^2 + c^2$. Prove that

$$1 + 2(abc)^n \geq a^{2n} + b^{2n} + c^{2n}$$

for all positive integers n.

Inequalities

Theorem (Holder's inequality)

Let $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ be nonnegative real numbers, and p, q positive real numbers such that $1/p + 1/q = 1$. Then

$$a_1 b_1 + \cdots + a_n b_n \leq (a_1^p + \cdots + a_n^p)^{1/p} (b_1^q + \cdots + b_n^q)^{1/q}$$

Inequalities

Theorem (Holder's inequality)

Let $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ be nonnegative real numbers, and p, q positive real numbers such that $1/p + 1/q = 1$. Then

$$a_1 b_1 + \cdots + a_n b_n \leq (a_1^p + \cdots + a_n^p)^{1/p} (b_1^q + \cdots + b_n^q)^{1/q}$$

Theorem (Jensen's inequality)

Let f be a convex function, and $x_1, \ldots, x_n$ real numbers in its domain. Then

$$f\left(\frac{x_1 + x_2 + \cdots + x_n}{n}\right) \leq \frac{f(x_1) + f(x_2) + \cdots + f(x_n)}{n}$$

with the inequality reversed if f is a concave function.

Group Theory

Theorem (Lagrange's Theorem)

Let G be a finite group of order n. Then any subgroup H of G has order dividing n.

Group Theory

Theorem (Lagrange's Theorem)

Let G be a finite group of order n. Then any subgroup H of G has order dividing n.

Theorem (Orbit-stabiliser theorem)

Let G be a finite group acting on a set X. The orbit of x is $G \cdot x = \{gx \mid g \in G\}$. and the stabiliser subgroup of g with respect to x is $G_x = \{g \in G \mid gx = x\}$.
Then $|G \cdot x||G_x| = |G|$.

Group Theory

Theorem (Lagrange's Theorem)

Let G be a finite group of order n. Then any subgroup H of G has order dividing n.

Theorem (Orbit-stabiliser theorem)

Let G be a finite group acting on a set X. The orbit of x is $G \cdot x = \{gx \mid g \in G\}$. and the stabiliser subgroup of g with respect to x is $G_x = \{g \in G \mid gx = x\}$.
Then $|G \cdot x||G_x| = |G|$.

Theorem ("Burnside's" lemma)

Let G be a finite group acting on a set X. The number of orbits $|X/G|$ of X is

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

where $X^g := \{x \in X \mid gx = x\}$ is the set of points fixed by g.

Examples

Example

Let r, s, t be positive integers which are pairwise relatively prime. If a and b are elements of an abelian group with unity element e, and $a^r = b^s = (ab)^t = e$, prove that $a = b = e$. Does the same conclusion hold if a and b are elements of an arbitrary non-commutative group?

Examples

Example

Let r, s, t be positive integers which are pairwise relatively prime. If a and b are elements of an abelian group with unity element e, and $a^r = b^s = (ab)^t = e$, prove that $a = b = e$. Does the same conclusion hold if a and b are elements of an arbitrary non-commutative group?

Example

Denote by S_n the group of permutations of the sequnece $(1, 2, \ldots, n)$. Suppose that G is a subgroup of S_n, such that for every $\pi \in G \backslash \{e\}$ there exists a unique $k \in \{1, 2, \ldots, n\}$ for which $\pi(k) = k$. Show that this k is the same for all $\pi \in G \backslash \{e\}$.

Examples

Example

Let r, s, t be positive integers which are pairwise relatively prime. If a and b are elements of an abelian group with unity element e, and $a^r = b^s = (ab)^t = e$, prove that $a = b = e$. Does the same conclusion hold if a and b are elements of an arbitrary non-commutative group?

Example

Denote by S_n the group of permutations of the sequnece $(1, 2, \ldots, n)$. Suppose that G is a subgroup of S_n, such that for every $\pi \in G \backslash \{e\}$ there exists a unique $k \in \{1, 2, \ldots, n\}$ for which $\pi(k) = k$. Show that this k is the same for all $\pi \in G \backslash \{e\}$.

Hint: Consider G acting on the set $X = \{1, 2, \ldots, n\}$ and apply orbit-stabiliser theorem.

Group theory

Example

Let G be a group of $n \geq 2$ be an integer. Let H_1 and H_2 be two subgroups of G that satisfy

$$[G : H_1] = [G : H_2] = n \quad \text{and} \quad [G : (H_1 \cap H_2)] = n(n-1).$$

Prove that H_1 and H_2 are conjugate in G.

Group theory

Example

Let G be a group of $n \geq 2$ be an integer. Let H_1 and H_2 be two subgroups of G that satisfy

$$[G : H_1] = [G : H_2] = n \quad \text{and} \quad [G : (H_1 \cap H_2)] = n(n-1).$$

Prove that H_1 and H_2 are conjugate in G.

Hint: Express H_1, H_2 both as the disjoint union of left cosets with respect to H_2 and and as the disjoint union of right cosets with respect to H_1.

Number Theory

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer n can be uniquely represented as a product of primes:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

up to ordering.

Number Theory

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer n can be uniquely represented as a product of primes:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

up to ordering.

Theorem (Bezout's identity)

Let a, b be two integers. Then there exist integers x, y such that $ax + by = gcd(a, b)$.

Number Theory

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer n can be uniquely represented as a product of primes:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

up to ordering.

Theorem (Bezout's identity)

Let a, b be two integers. Then there exist integers x, y such that $ax + by = gcd(a, b)$.

Theorem

Let $a > 1$ be a positive integer, and let m, n be a positive integer. Then

$$gcd(a^m - 1, a^n - 1) = a^{gcd(m,n)} - 1$$

Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem)

Let $m_1, \ldots, m_k$ be pairwise coprime positive integers. Let $c_1, \ldots, c_k$ be integers. Then the system of congruences

$$\begin{aligned} x &\equiv c_1 \ (mod\ m_1) \\ x &\equiv c_2 \ (mod\ m_2) \\ &\vdots \\ x &\equiv c_k \ (mod\ m_k) \end{aligned}$$

has a unique solution mod $m_1 m_2 \cdots m_k$.

Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem)

Let $m_1, \ldots, m_k$ be pairwise coprime positive integers. Let $c_1, \ldots, c_k$ be integers. Then the system of congruences

$$\begin{aligned} x &\equiv c_1 \ (mod\ m_1) \\ x &\equiv c_2 \ (mod\ m_2) \\ &\vdots \\ x &\equiv c_k \ (mod\ m_k) \end{aligned}$$

has a unique solution mod $m_1 m_2 \cdots m_k$.

- Equivalently, let $M = m_1 m_2 \cdots m_k$. Then there's a ring isomorphism given by:

$$\begin{aligned} \mathbb{Z}/M\mathbb{Z} &\longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \\ x \bmod M &\longmapsto (x \bmod m_1, \ldots, x \bmod m_k) \end{aligned}$$

Chinese Remainder Theorem

Example

Find the number of positive integers x satisfying the following two conditions:

1. $x < 10^{2006}$.
2. $x^2 - x$ is divisible by 10^{2006}.

Chinese Remainder Theorem

Example

Find the number of positive integers x satisfying the following two conditions:

1. $x < 10^{2006}$.
2. $x^2 - x$ is divisible by 10^{2006}.

Example

Let p and q be relatively prime positive integers. Prove that

$$\sum_{k=0}^{pq-1} (-1)^{\left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{q} \right\rfloor} = \begin{cases} 0 & \text{if } pq \text{ is even,} \\ 1 & \text{if } pq \text{ is odd.} \end{cases}$$

Number Theory

Theorem (Wilson's Theorem)

If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.

Number Theory

Theorem (Wilson's Theorem)

If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.

Theorem (Fermat's Little Theorem)

Let p be a prime, and a an integer not divisible by p. Then $a^{p-1} \equiv 1 \pmod{p}$.

Number Theory

Theorem (Wilson's Theorem)

If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.

Theorem (Fermat's Little Theorem)

Let p be a prime, and a an integer not divisible by p. Then $a^{p-1} \equiv 1 \pmod{p}$.

Example

Let p be a prime number. Prove that

$$x^{p^p-1} - 1 = (x^p - x + 1)f(x) + pg(x)$$

for some polynomial f and g with integer coefficients

Number Theory

Euler's function

Let n be a positive integer. The Euler function $\varphi(n)$ is the number of positive integers less than n coprime to n. It holds that

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right),$$

where $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is the factorization of n into primes.

Number Theory

Euler's function

Let n be a positive integer. The Euler function $\varphi(n)$ is the number of positive integers less than n coprime to n. It holds that

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right),$$

where $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is the factorization of n into primes.

Theorem (Euler's theorem)

Let n be a positive integer, and a an integer coprime to n. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$