Matematica del discreto

Relazioni

Una relazione binaria tra X e Y è un insieme di coppie ordinate $(x,y) \in X \times Y$. Una relazione può essere:

Riflessiva	xRx
Simmetrica	$xRy \Rightarrow yRx$
Antisimmetrica debole	$xRy \wedge yRx \Rightarrow x = y$
Antisimmetrica forte	$xRy \Rightarrow \neg yRx$
Transitiva	$xRy, yRz \Rightarrow xRz$
Equivalenza	riflessiva, simmetrica e transitiva
Ordine debole	antisimmetrica debole e transitiva
Ordine forte	antisimmetrica forte e transitiva

Equazioni diofantee

L'equazione $ax + by = d$ ha soluzione se e solo se d è multiplo di mcd(a,b), le infite soluzioni hanno la forma $(x + kb/d, y - ka/d)$.
Per risolvere $ax + by = d$ basta risolvere $ax_1 + by_1 = c = \text{mcd}(a,b)$, $x = x_1 d/c, y = y_1 d/c$

Congruenze lineari

$ax \equiv 1 (\text{mod } n)$ ha soluzione se e solo se a è coprimo con n, la soluzione è $x \equiv a^{\varphi(n)-1} (\text{mod } n)$.

Teorema del resto cinese

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ \vdots \\ x \equiv b_k \pmod{n_1} \end{cases} \qquad \begin{array}{l} N_i = \prod_{j \neq i} n_i \\ N_i y_i \equiv 1 \pmod{n_i} \\ x \equiv \sum b_i y_i N_i \pmod{\prod n_i} \end{array}$$

Phi di Eulero

$\varphi(p^k) = p^k - p^{k-1}$
$\varphi(n) = \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \dots \varphi(p_r^{k_r})$

Gruppi

Data struttura algebrica G e una leggere di composizone $\times$, $(G, \times)$ è un gruppo se:

Associativa	$(v \times w) \times z = v \times (w + z)$
Elemento neutro	$v \times 1 = v$
Elemento inverso	$\exists x \quad v \times x = 1$

Un gruppo è abeliano se: $v \times w = w \times v$

Anelli e campi

$(A, +, \times)$ è un anello se:
- $(A, +)$ è un gruppo abeliano;
- $(A, \times)$ è un monoide;
- vale la proprietà distributiva del prodotto rispetto alla somma.

L'insieme degli elementi invertibili di un anello forma un gruppo
Un elemento $a \neq 0$ si dice divisore dello zero se $\exists b$ tc $a \times b = 0$.
Un campo è un anello abeliano in cui ogni elemento è invertibile.

Gruppi di permutazione

Un gruppo di permutazione è l'insieme delle applicazioni bigettive su un insieme X.

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} \quad \sigma = \begin{pmatrix} a_1 & \sigma(a_1) & \sigma(\sigma(a_1)) & \dots \end{pmatrix}$$

Due cicli sono disgiunti (permutano) se operano su insiemi disgiunti.
L'ordine di un ciclo è il più piccolo m tale che $\sigma^M = I$.
Teorema di Lagrange: l'ordine di un sottogruppo H di un gruppo G è un divisore dell'ordine di G.
Un sottogruppo ciclico è l'insieme: $\{1, x, x^2, \dots, x^n\}$.
Un gruppo G è ciclico se tutti gli elementi possono essere espressi come potenza di $x \in G$, x è un generatore di G.
Se un gruppo è ciclico ogni su sottogruppo è ciclico.
Se un gruppo è ciclico di ordine n, per ogni divisore d di n, esiste ed è unico un sottogruppo di ordine d.

Determinante

$\det : M_{n,n}(K) \to K$

$n = 1 \quad A = [a] \quad \det A = a$

$n > 1 \quad$ Ricorsivamente
- A_{ij} ottenuta da A togliendo riga i e colonna j
- $M_{ij} = \det A_{ij}$ (detto minore complementare)
- $C_{ij} = (-1)^{i+j} M_{ij}$ (detto complemento algebrico)
- $\det A = \sum_{i=1}^n a_{1i} C_{1i}$

Th di Laplace: si può usare una riga o una colonna qualsiasi.
- $\det A = \det A^T$
- Se una riga o colonna ha tutti zeri: $\det A = 0$
- Se si scambiano 2 righe: $\det A' = -\det A$
- Se due righe sono uguali: $\det A = 0$
- Moltiplicando una riga: $\det A' = k \det A$, $\det kA = k^n \det A$
- Sommando ad una riga un'altra riga: $\det A' = \det A$
- In una matrice triangolare: $\det A = \prod_{i=1}^n a_{ii}$
- Teorema di Binet: $\det AB = \det A \cdot \det B$
- A è inveribile se e solo se: $\det A \neq 0$
- Se A è invertibile allora: $\det A^{-1} = (\det A)^{-1}$

Sistemi lineari

$$\begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + \dots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + \dots + a_{mn}x_n = b_m \end{cases} \qquad A|b = \left[\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & b_1 \\ a_{21} & \cdots & a_{2n} & b_2 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{array}\right]$$

Rango

Minore di ordine p: il determinate di una sottomatrice quadrata di ordine p.
Rango: il più grande p tale che esista un minore di ordine p non nullo, è uguale al numero di pivot durante GJ.

Autovalori e autovettori

$v \neq 0$ è autovettore di autovalore λ se $Av = \lambda v$
Per trovare gli autovalori risolvere $\det(A - \lambda I) = 0$.
Il determinante $p(\lambda)$ viene chiamato *polinomio caratteristico*.
Per trovare gli autovalori risolvere $(A - \lambda I)v = 0$.
Molteciplità algebrica m_a: molteciplità di λ in $p(\lambda)$.
Molteciplità geometrica m_g: $\dim(\ker(A - \lambda I))$.

Matrici simili

Due matrici A, B sono simili se $\exists M$, $A = MBM^{-1}$, due matrici sono simili se rappresentano uno stesso omomorfismo in basi diverse.
Due matrici simili hanno gli stessi autovalori, lo stesso determiante e lo stesso rango.

Spazi vettoriali

Uno spazio vettoriale su un campo $\mathbb{K}$ è un insieme V su cui è definita una somma e un prodotto scalare tale che:
- $(V,+)$ è un gruppo abeliano
- $k(v + w) = kv + kw$
- $(k_1 + k_2)v = k_1 v + k_2 v$
- $1 \times v = v$

W è un sottospazio vettoriale di V se W è chiuso per combinazioni lineari: $k_1 w_1 + k_2 w_2 \in W$
Span(I): insieme delle combinazioni lineari di I.
Uno sv è finitamente generato se $\exists I \subseteq V$ tale che $V = \text{Span}(I)$, I è un insiemi di generatore per V.
I è linearmente indipendente se esiste un unico modo di generare 0.
Una base è un insieme di generatori linearmente indipendente.
Tutte le basi hanno la stessa cardinalita, detta dimensione.
Th di Grassman: $\dim(S) + \dim(T) = \dim(S \cap T) + \dim(S + T)$

Omomorfismo

Un omomorfismo è una funzione $f \colon V \to W$ tale che: $f(hv + kw) = hf(v) + kf(w)$.
$\ker f = \{v \in V \mid f(v) = 0\}$
$\text{Im} f = \{w \in W \mid \exists v, w = f(v)\}$
$\ker f$ e $\text{Im} f$ sono sottospazi vettoriali rispettivamente di V e W.
Se V è generato da $\{v_1, \dots\}$ allore $\text{Im} f$ è generato da $\{f(v_1), \dots\}$.
Teorema nullità più rango: $\dim V = \dim(\ker f) + \dim(\text{Im} f)$.
Iniettivo: $f(v) = f(w) \Leftrightarrow v = w$.
Surgettivo: $\text{Im} f = W$.
Isomorfismo: sia iniettivo che surgettivo.

Omomorfismi mediante matrici

$\mathbb{V} = \{v_1, \dots, v_n\}$ base di V, $\mathbb{W} = \{w_1, \dots, w_m\}$ base di W

$$\begin{array}{c} f(v_1) = a_{11}w_1 + \dots + a_{1m}w_m \\ \vdots \\ f(v_n) = a_{11}w_1 + \dots + a_{nm}w_m \end{array} \to A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}$$

$\dim(\text{Im} f) = \text{rg}(A)$

Diagonalizzazione

Una matrice si dice diagonalizzabile se è simile ad una matrice diagonale.
Una matrice è diagonalizzabile se:
- $\sum m_a(a_i) = n$, non ci sono soluzioni complesse
- $m_g(a_i) = m_a(a_i) \Longleftrightarrow n - \text{rg}(A - a_i I) = m_a(a_i)$

Vettori

Vettore: $\overrightarrow{v} = (v_1, v_1, \dots, v_n)$
Norma: $||\vec{v}|| = \sqrt{v_1^2 + v_2^2 + \dots + v_n^2}$
Prodotto scalare: $\overrightarrow{v}\overrightarrow{w} = \sum_{i=1}^n v_i w_i = ||\overrightarrow{v}|| \cdot ||\overrightarrow{w}|| \cos\theta$
Angolo tra vettori: $\cos\theta = \frac{\overrightarrow{v} \cdot \overrightarrow{w}}{||\overrightarrow{v}|| \cdot ||\overrightarrow{w}||}$
Perpendicolari: $\overrightarrow{v}\overrightarrow{w} = 0$
Paralleli: $\overrightarrow{v} = k\overrightarrow{w}$

Rette in 2D

Forma cartesiana: $r\colon ax + by + c = 0$
Forma parametica: $r\colon P + t\overrightarrow{v}$
Da parametrica a cartesiana: $\begin{cases} x = p_x + tv_x \\ y = p_y + tv_y \end{cases}$
Da cartesiana a parametrica: $(0, -c/b) + t(1, -a/b)$

Rette in 3D

Forma cartesiana: $\begin{cases} ax_1 + by_1 + cz_1 + d_1 = 0 \\ ax_2 + by_2 + cz_2 + d_2 = 0 \end{cases}$
Forma parametica: $r\colon P + t\overrightarrow{v}$
Da parametrica a cartesiana: $\begin{cases} x = p_x + tv_x \\ y = p_y + tv_y \\ z = p_z + tv_y \end{cases}$
Da cartesiana a parametrica:
F.C. $\Longrightarrow \begin{cases} y = m_1 x + q_1 \\ z = m_2 x + q_2 \end{cases} \Longrightarrow r\colon \begin{pmatrix} 0 \\ q_1 \\ q_2 \end{pmatrix} + t \begin{pmatrix} 1 \\ m_1 \\ m_2 \end{pmatrix}$

Piani in 3D

Forma cartesiana: $ax + by + cz + d = 0$
Forma parametica: $\pi\colon P + t\overrightarrow{v} + s\overrightarrow{w}$

Basato sul corso *Matematica del discreto* A.A. 2020/2021 del docente Luperi Baglini Lorenzo.