Vettori

Combinazione lineare: Un vettore $y \in R^n$ si dice combinazione lineare dei vettori $v_1, ..., v_k$ se esistono k moltiplicatori reali $w_1, ..., w_k$ tali che $v = \sum_{i=1}^{k} w_i v_i$.

Ovvero, un vettore è combinazione lineare di altri vettori se il vettore è il risultato della somma degli altri vettori, ognuno di questi moltiplicato per una costante qualsiasi.

Vettori linearmente indipendenti: Un insieme di vettori è indipendente se è possibile ottenere il vettore nullo solamente con tutti i coefficienti w_i uguali a 0.

Esempio: $\{(1, 0), (0, 1)\}$.

Vettori linearmente dipendenti: Un insieme di vettori è dipendente se è possibile ottenere il vettore nullo con almeno un coefficiente w_i diverso da 0.

Un insieme che contiene il vettore nullo è linearmente dipendente.

Esempio: $\{(1, 1), (2, 2)\}$.

Applicazioni lineari

Una applicazione lineare o trasformazione lineare è:

- una funzione lineare tra due spazi vettoriali sullo stesso campo,
- ovvero una funzione che conserva le operazioni di somma di vettori e di moltiplicazione per uno scalare,
- ovvero una trasformazione lineare che preserva le combinazioni lineari,
- ovvero un omomorfismo di spazi vettoriali, in quanto conserva le operazioni che caratterizzano gli spazi vettoriali.

Condizione di linearità: $\forall \alpha, \beta \in \mathbb{K}$ e $\forall v_1, v_2 \in V$ vale $f(\alpha v_1 + \beta v_2) = \alpha f(v_1) + \beta f(v_2)$.

Notazione matriciale: Siano il vettore $v \in \mathbb{R}^n$ e $A = Mat(m, n, \mathbb{R})$, un'applicazione lineare $f \colon \mathbb{R}^n \to \mathbb{R}^m$ si indica con $f(v) = Av$.

$$\begin{aligned} f(v) &= f(x_1, \ldots, x_n) \\ &= (a_{11}x_1 + \cdots + a_{1n}x_n,\ \ldots\ , a_{m1}x_1 + \cdots + a_{mn}x_n) \\ &= Av = \begin{bmatrix} a_{11}x_1 + \cdots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n \end{bmatrix} = \begin{bmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \ldots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}. \end{aligned}$$

Dalla definizione ne deriva che:

- il numero di righe è dato dal numero di variabili del dominio;
- il numero di colonne è dato dal numero di variabili del codominio.

Matrice canonica: Con $f(e_1) = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix}$, $f(e_2) = \begin{pmatrix} a_2 \\ b_2 \end{pmatrix}$ ed $f(e_3) = \begin{pmatrix} a_3 \\ b_3 \end{pmatrix}$ i vettori (linearmente indipendenti) della base canonica dell'applicazione lineare $f : \mathbb{R}^3 \to \mathbb{R}^2$, allora se $v = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ è il vettore generico di $\mathbb{R}^3$:

$$\begin{aligned} f(v) = f\begin{pmatrix} x \\ y \\ z \end{pmatrix} &= f(xe_1 + ye_2 + ze_3) = xf(e_1) + yf(e_2) + zf(e_3) = x\begin{pmatrix} a_1 \\ b_1 \end{pmatrix} + y\begin{pmatrix} a_2 \\ b_2 \end{pmatrix} + z\begin{pmatrix} a_3 \\ b_3 \end{pmatrix} \\ &= \begin{pmatrix} a_1x + a_2y + a_3z \\ b_1x + b_2y + b_3z \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}. \end{aligned}$$

La matrice A è detta matrice canonica di f, ed ha colonne $\begin{pmatrix} f(e_1) & \cdots & f(e_n) \end{pmatrix}$.

Esempio: Sia $f : \mathbb{R}^3 \to \mathbb{R}^3$ definita come segue:

$$f(0,1,1) = (5,2,3);$$
$$f(2,0,0) = (2,2,0);$$
$$f(1,1,0) = (2,1,1);$$

La matrice rappresentativa dell'applicazione lineare va espressa tramite la base canonica, che quindi va ricavata.

$$f(1,0,0) = f(2,0,0)/2 = (2,2,0)/2 = \underline{(1,1,0)};$$
$$f(0,1,0) = f(1,1,0) - f(1,0,0) = (2,1,1) - (1,1,0) = \underline{(1,0,1)};$$
$$f(0,0,1) = f(0,1,1) - f(0,1,0) = (5,2,3) - (1,0,1) = \underline{(4,2,2)}.$$

A questo punto la matrice rappresentativa è espressa con i vettori immagine in colonna.

$$A = \begin{pmatrix} 1 & 1 & 4 \\ 1 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix}.$$

Esempio: La matrice rappresentativa (rispetto alle basi canoniche) dell'applicazione lineare definita da $f(x,y,z) = (2x + 3y - z, 4x + 27y - 5z)$ è

$$A = \begin{pmatrix} 2 & 3 & -1 \\ 4 & 27 & -5 \end{pmatrix}.$$

Matrici

Matrice triangolare superiore: La riduzione di una matrice a scala tramite il metodo di eliminazione di Gauss genera una matrice triangolare superiore con medesime soluzioni della matrice originale. È utile per:

- risolvere sistemi lineari del tipo $Ax = b$;
- determinare il rango di una matrice (contando gli elementi di pivot non nulli).

Determinante: Se il determinante di una matrice di vettori è diverso da 0 allora i vettori sono linearmente indipendenti.

Rango di una matrice: Si definisce rango di una matrice il massimo numero di vettori riga linearmente indipendenti tra loro o, equivalentemente, il massimo numero di vettori colonna linearmente indipendenti.

Rango massimo: Una matrice di m righe per n colonne può avere rango al massimo uguale a $min(m,n)$. Se il rango coincide con $min(m,n)$ allora è massimo.

Matrice invertibile: Una matrice è invertibile se e solo se ha rango massimo, quindi determinante diverso da 0.

[HOWTO] Calcolo del rango: È possibili determinare il rango di una matrice tramite:

- il criterio dei minori;
- il metodo di eliminazione di Gauss.

Minori di ordine j: Data una matrice di m righe per n colonne, un suo minore di ordine j è una qualsiasi sottomatrice quadrata di ordine j, con $1 \leq j \leq min(m,n)$.

[HOWTO] Criterio dei minori: j_i in prima istanza è $min(m,n)$.
Se c'è almeno un minore di ordine j_i con determinante diverso da 0 allora il rango della matrice originale è j_i. Se tutti i minori di ordine j_i hanno determinante uguale a 0 allora il rango della matrice è dato da j_{i+1}. L'i-esimo minore j_i, tranne il primo, ha ordine $j_{i-1} - 1$.

[HOWTO] Eliminazione di Gauss: $R_i = R_i - \frac{a_i}{a_p} R_p$ dove i è la riga corrente e p è la riga di pivot.

Se a_i è 0 si salta la riga essendo già a scalino e si procede con la successiva.

Se l'elemento di pivot a_p è 0 si scambia la riga con un'altra il cui elemento di pivot è diverso da 0.

Sistema di generatori

Un sistema di generatori è un insieme di vettori che permette di ottenere tutti i vettori dello spazio mediante opportune combinazioni lineari. Con V uno spazio vettoriale, v, v_1, v_n, vettori appartenenti a V e $a_1 \dots a_n$ degli scalari appartenenti al campo K:

$$v = a_1v_1 + a_2v_2 + \dots + a_nv_n = \sum_{i=1}^{n} a_iv_1$$

Dato uno spazio vettoriale qualsiasi, non esiste un solo sistema di generatori.
Per ogni spazio $V \neq 0$ esistono infiniti sistemi di generatori.

Basi e generatori:

- Una base di uno spazio vettoriale è sempre un sistema di generatori;
- Un sistema di generatori non è necessariamente una base.

[HOWTO] Verifica di un sistema di generatori: Un insieme di vettori è un sistema di generatori se la matrice (del sistema lineare associato all'insieme di vettori) ha rango massimo. Se non ha rango massimo non è un sistema di generatori.

Esempio:

$$\{[1,0,1],[0,0,3],[1,2,1],[1,-1,0]\}$$
$$w = x_1[1,0,1] + x_2[0,0,3] + x_3[1,2,1] + x_4[1,-1,0]$$
$$[a,b,c] = x_1[1,0,1] + x_2[0,0,3] + x_3[1,2,1] + x_4[1,-1,0]$$
$$[a,b,c] = [x_1,0,x_1] + [0,0,3x_2] + [x_3,2x_3,x_3] + [x_4,-x_4,0]$$
$$[a,b,c] = [x_1 + x_3 + x_4, 2x_3 - x_4, x_1 + 3x_2 + x_3]$$
$$\begin{cases} x_1 + x_3 + x_4 = a \\ 2x_3 - x_4 = b \\ x_1 + 3x_2 + x_3 = c \end{cases}$$
$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 2 & -1 \\ 1 & 3 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} a \\ b \\ c \end{bmatrix}$$

Il rango è uguale a 3, è massimo e quindi l'insieme di vettori è un sistema di generatori.

Spazio vettoriale

Base di uno spazio vettoriale: Un insieme di vettori B è una base dello spazio vettoriale V se B:

- è un sistema di generatori di V;
- è un sistema di vettori linearmente indipendenti.

Dimensione dello spazio: La dimensione dello spazio vettoriale V, indicata con $dim(V)$, è il numero di elementi di una base qualsiasi di V.
Sottospazio generato

Basi derivate da altre basi: Disponendo di una base B per lo spazio vettoriale V, tutte le basi che si ottengono moltiplicando i vettori di B per scalari non nulli sono ancora basi di V (distinte da B).

Teorema dell'esistenza di una base: Ogni spazio vettoriale ammette l'esistenza di una base.

Teorema della non unicità della base: Ogni spazio vettoriale ammette infinite basi (se il campo di scalari è infinito).

Cardinalità delle basi: Ogni base di uno spazio vettoriale V ha la stessa cardinalità, ovvero lo stesso numero di elementi. $\forall B, B'$ basi di $V \implies |B| = |B'|$

Da ciò, qualsiasi sistema di generatori avente un numero di vettori superiore alla dimensione dello spazio vettoriale non può costituire una base dello spazio stesso.

Base di uno spazio vettoriale: Una base di $\mathbb{R}^n$ è costituita esattamente da n vettori.

Base canonica di uno spazio vettoriale: La base canonica di $\mathbb{R}^n$ è costituita esattamente da n vettori ognuno dei quali ha una sola componente non nulla, ed ognuna di queste componenti non nulle è in una posione nel vettore diversa da tutti gli altri vettori.

Esempio: Base canonica per $\mathbb{R}^3 = \{\{1,0,0\},\{0,1,0\},\{0,0,1\}\}$.

[HOWTO] Estrarre una base da un sistema di generatori tramite il metodo di eliminazione di Gauss:

1. si popola la matrice M con i vettori generatori (disposti per colonna);
2. si riduce la matrice M tramite il metodo di eliminazione di Gauss ottenendo una mtrice M';
3. le colonne di M' con pivot indicano in M (la matrice originale) le colonne che costituiscono una base.

[HOWTO] Estrarre una base da un sistema di generatori tramite il criterio dei minori:

1. si popola la matrice M con i vettori generatori (disposti per colonna);
2. si usa il criterio dei minori per trovare una sottomatrice M' con $det(M') \neq 0$;
3. le colonne di M' indicano in M (la matrice originale) le colonne che costituiscono una base; le colonne di M si prendono per intero anche se le righe di M' sono minori di M.

Autovalore e autovettore:

Un numero complesso (o anche reale) λ è un autovalore dell'endomorfismo $f : V \to V$, con V uno spazio vettoriale su $\mathbb{R}$, A_f la matrice associata-ad/rappresentativa-di f rispetto ad una base di V e I la matrice identità diagonale:

- se esiste un vettore $v \in V$ tale che $f(v) = \lambda v$;
- oppure se $A_f v = \lambda v$;
- oppure se $A_f - \lambda I$ non è invertibile, ovvero $det(A_f - \lambda I) = 0$.

Ovvero un vettore v è un autovettore se differisce dalla sua immagine mediante f solo per un multiplo scalare c. In questo contesto v è un autovettore dell'autovalore c.

Dire autovetorre ed autovalore della matrice A_f significa autovettore ed autovalore dell'endomorfismo f che ha A_f come matrice associata/rappresentativa.

[HOWTO] Trovare l'autovalore e l'autovettore: Una matrice per non essere invertibile deve avere determinante uguale a 0. Per cui:

$$det(A_f - \lambda I) = 0$$

In particolare il determinante della matrice A_f è un polinomio in λ detto polinomio caratteristico della matrice A_f. Gli autovalori della matrice sono gli zeri del polinomio caratteristico.

Matrice da vettori immagine

Matrice rispetto a due basi

Immagine

Sia $F : D_{ominio} \to C_{odominio}$ un'applicazione lineare definita tra spazi vettoriali su un campo $\mathbb{K}$ (ad esempio $\mathbb{R}$), definiamo immagine di F:

$$Im(F) = \{i \in C \mid \exists v \in D \text{ per cui } F(v) = i\}.$$

[HOWTO] Come calcolare $dim(Im(F))$: I vettori che costituiscono la matrice rappresentativa di un'applicazione lineare, indipendentemente dalla base a cui essi sono riferiti, costituiscono un sistema di generatori.

Per calcolare $dim(Im(F))$ si può:

- estrarre una base da un suo sistema di generatori e determinarne la dimensione;
- calcolare il rango di un suo sistema di generatori.

Nucleo o kernel

Sia $F: D_{ominio} \to C_{odominio}$ un'applicazione lineare definita tra spazi vettoriali su un campo $\mathbb{K}$ (ad esempio $\mathbb{R}$), definiamo il nucleo di F:

$$Ker(F) = \{v \in D \mid F(v) = \underline{0} \in C\}$$

Ovvero è l'insieme degli elementi del dominio che hanno immagine $\underline{0}$ mediante un'applicazione lineare definita su spazi vettoriali su un campo.

Esempio: Sia $F: \mathbb{R}^4 \to \mathbb{R}^2$ definita da $A = \begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \end{pmatrix}$, allora $Ker(F) \subset \mathbb{R}^4$ ed è il sottoinsieme di vettori x soluzione del sistema omogeneo $Ax = 0$.

[HOWTO] Calcolo di $dim(Ker(F))$: Sia A la matrice associata all'applicazione lineare F, per calcolare $dim(Ker(F))$ è sufficiente trovare i vettori soluzione del sistema di equazioni $Ax = 0$. I vettori soluzione (anche solo uno) costituiscono una base del nucleo e la dimensione di questa base è la dimensione del nucleo.

Dimensione: Essendo il nucleo un sottospazio del dominio, ne deriva che $0 \leq dim(Ker(F)) \leq dim(D)$.

- Se $dim(Ker(F)) = 0$, allora l'unico elemento del nucleo è $\underline{0}$.
- Se $dim(Ker(F))) = dim(D)$, allora $Ker(F) = D$ ed F è l'applicazione lineare che associa ad ogni elemento di D lo zero di C.

Teorema dell'iniettività: F è iniettiva se e solo se $Ker(F) = \{\underline{0}\}$, ovvero se e solo se F ha nucleo banale.

Teorema di nullità più rango (o teorema del rango o teorema della dimensione):

$$dim(D) = dim(Ker(F)) + dim(Im(F))$$

Equazioni diofantee

Minimo comune multiplo (mcm): $\dfrac{a \times b}{MCD(a,b)}$.

Massimo comune divisore (MCD) (algoritmo di Euclide):

$a = qb + r$.

$$MCD(N,n): \quad \begin{aligned} \mathrm{N} &= \mathrm{n} * q_1 + r_1 \\ \mathrm{n} &= r_1 * q_2 + r_2 \\ r_1 &= r_2 * q_3 + r_3 \\ \ldots &= \ldots * \ldots + \ldots \\ r_h &= r_{h+1} * q_{h+2} + r_{h+2} \\ r_{h+1} &= r_{h+2} * r_{h+1} + \underline{0} \end{aligned} \quad \Longrightarrow \quad r_{h+2}.$$

Teorema di Bézout: Se a, b sono interi e (a,b) è il loro massimo comune divisore, allora esistono interi h, k tali che

$$ha + kb = (a,b).$$

Esempio: $132h + 51k = 3$

$$MCD(132,51): \quad \begin{aligned} 132 &= 51 * 2 + 30\ ; \\ 51 &= 30 * 1 + 21\ ; \\ 30 &= 21 * 1 + 9\ ; \\ 21 &= 9 \ \ * 2 + 3\ ; \\ 9 &= 3 \ \ * 3 + \underline{0}\ ; \end{aligned} \quad \Longrightarrow \quad \begin{aligned} \underline{3} &= 21 - 2\cdot 9 \\ &= 21 - 2(30-21) \\ &= -2\cdot 30 + 3\cdot 21 \\ &= -2\cdot 30 + 3(51-30) \\ &= 3\cdot 51 - 5\cdot 30 \\ &= 3\cdot 51 - 5(132 - 2\cdot 51) \\ &= \underline{13\cdot 51 - 5\cdot 132}. \end{aligned}$$

Permutazioni

Con S_n si intende l'insieme di permutazioni composte dai numeri che vannno da 1 a n.

Se in una permutazione non compare un numero, questo vuol dire che va in se stesso.

Numeri complessi

Forma cartesiana :

$$z = x + iy \quad \text{dove} \quad Re(z) = x,\ Im(z) = y.$$

Forma esponenziale: $z = |z|\ (\cos\theta + i\ \sin\theta)$

Dove $x = Re(z) = |z|cos\theta$ e $y = Im(z) = |z|sin\theta$.

Modulo: $r = |z| = \sqrt{x^2 + y^2}$.

Argomento: $\theta = Arg(z) \in (-\pi, +\pi] = \begin{cases} \arccos\left(\dfrac{x}{|z|}\right) & \text{se } y \geq 0 \\ -\arccos\left(\dfrac{x}{|z|}\right) & \text{se } y < 0 \end{cases} = \begin{cases} \frac{\pi}{2} \text{ se } x = 0,\ y > 0 \\ -\frac{\pi}{2} \text{ se } x = 0,\ y < 0 \\ \text{non definito se } x = 0,\ y = 0 \\ \arctan\left(\frac{y}{x}\right) \text{ se } x > 0,\ y \text{ qualsiasi} \\ \arctan\left(\frac{y}{x}\right) + \pi \text{ se } x < 0,\ y \geq 0 \\ \arctan\left(\frac{y}{x}\right) - \pi \text{ se } x < 0,\ y < 0 \end{cases}$

$$\theta = Arg(z) \in [0, 2\pi) = \begin{cases} \frac{\pi}{2} \text{ se } x = 0,\ y > 0 \\ \frac{3\pi}{2} \text{ se } x = 0,\ y < 0 \\ \text{non definito se } x = 0,\ y = 0 \\ \arctan\left(\frac{y}{x}\right) \text{ se } x > 0, y \geq 0 \\ \arctan\left(\frac{y}{x}\right) + 2\pi \text{ se } x > 0, y < 0 \\ \text{TODO: manca una condizione} \end{cases}$$

Calcolo delle radici di un numero complesso

Gruppi

Un gruppo $(G, *)$ è una coppia composta da un insieme G ed un'operazione $*$ su G che:

- risulti essere associativa, ovvero $(a * b) * c = a * (b * c)$;
- ammetta un elemento neutro i, ovvero $g * i = i * g = g \quad \forall g \in G$;
- rispetto alla quale ogni elemento di G risulti invertibile, ovvero $a * a_{inv} = i$.

Un gruppo la cui operazione è commutativa è detto gruppo abeliano.

Un sottogruppo di un gruppo deve godere delle stesse proprietà del gruppo, più:

$$\forall a, b \in S \subseteq G \quad a * b \in S$$

Anelli

Un insieme $(A, +, \times)$ dotato di due operazioni, dette somma e prodotto, è detto anello se:

- $(A, +)$ è un gruppo abeliano con elemento neutro 0_A;
- $\times$ è associativa con elemento neutro 1_A;
- vale la legge distributiva del prodotto rispetto alla somma: $\forall a, b, c \in A \quad a \times (b + c) = a \times b + a \times c$ e $(b + c) \times a = b \times a + c \times a$;
- $0_A \neq 1_A$.

Campi

Un insieme $(C, +, \times)$ dotato di due operazioni, dette somma e prodotto, è detto campo se:

- $(C, +)$ è un gruppo abeliano con elemento neutro 0_C;
- $(C, \times) \backslash \{0_C\}$ è un gruppo abeliano con elemento neutro 1_C;
- vale la legge distributiva del prodotto rispetto alla somma: $\forall a, b, c \in C \quad a(b + c) = ab + ac$ e $(b + c)a = ba + ca$.

Omomorfismi

Dati due gruppi G e G',
un **omomorfismo** è una funzione $f : G \to G'$ tale che

$$f(ab) = f(a)f(b).$$

Dati due gruppi $(G, +)$ e $(G', \times)$,
un **omomorfismo di gruppi** è una funzione $f : G \to G'$ tale che $\forall a, b \in G$

$$f(a + b) = f(a) \times f(b).$$

Dati due anelli $(A, +, \times)$ e $(A', +', \times')$,
un **omomorfismo di anelli** è una funzione $f : A \to A'$ tale che $\forall a, b \in A$

$$f(a + b) = f(a) +' f(b),$$
$$f(a \times b) = f(a) \times' f(b).$$

Se loperazione di prodotto definita in A gode della proprietà commutativa diremo che A è un anello commutativo.

Isomorfismi: Un isomorfismo è un omomorfismo biettivo.
Un esempio sono le matrici triangolari superiori.

Teorema fondamentale dell'isomorfismo: Dati due gruppi G, G', un sottogruppo normale N di G ed un omomorfismo $f : \ G \to G'$ con nucleo $Ker(f) = N$, esiste un unico isomorfismo $\overline{f} : \ G/N \to f(g) \mid f = \overline{f}(\pi(x))$. In particolare l'immagine di f è un gruppo isomorfo a G/N.

Immagine: È l'immagine $\in G'$ dell'applicazione lineare su G.

Nucleo: È l'insieme degli elementi $\in G$ che tramite l'applicazione lineare vengono trasformati nell'identità di G'.

Partizioni

Una partizione di un insieme è una suddivisione dell'insieme in sottoinsieme disgiunti.

Relazioni di equivalenza

Una relazione di equivalenza è una relazione che soddisfa le seguenti proprietà:

(transitiva) se $a \sim b$ e $b \sim c$, allora $a \sim c$;

(simmetrica) se $a \sim b$ allora $b \sim a$;

(riflessiva) $a \sim a \quad \forall a \in S$.

Classi di equivalenza: Un sottoinsieme di A che contiene tutti e soli gli elementi equivalenti a un qualche elemento $x \in A$ prende il nome di classe di equivalenza di x per la relazione $\sim$ e si indica con $[x]_\sim$. In una classe di equivalenza tutti gli elementi in essa contenuti sono tra loro equivalenti.

Sia G un gruppo e H un suo sottogruppo normale ($gH = Hg$), $[g] = Hg = gH = [g]^*$.

Classi laterali

Laterale destro: $Hx = \{hx \mid h \in H \text{ e } x \in Hx\}$

Laterale sinitro: $xH = \{xh \mid h \in H \text{ e } x \in xH\}$

Se H è un insieme finito si ha che $|H| = |Hx| = |xH| \quad \forall x \in G$.

Teorema di Lagrange: Se G è un gruppo finito ed H un suo sottogruppo allora $|G| = r|H|$ dove r è il numero dei laterali destri o sinistri di H in G. Ovvero l'ordine di H divide l'ordine di G.

Le classi laterali sono classi di equivalenza rispetto alla relazione di congruenza:

$$a \equiv b, \text{ se } b = ah \text{ per qualche } h \in H$$

e costituiscono una partizione del gruppo.

Gruppi quoziente

L'insieme delle classi di equivalenza su A si chiama insieme quoziente di A per la relazione $\sim$, e viene indicato con l'espressione $A/\sim$.

Sia G un gruppo ed H un sottogruppo di G, $G/H = \{[g] \mid g \in G\}$.

Congruenze

Dato un intero positivo n, due numeri interi a, b sono congrui modulo n, indicati con $a \equiv b \mod n$, se $a - b$ è divisibile per n, ovvero se esiste un numero intero h tale che $a - b = hn$.

Proprietà elementari:

1. se $a \equiv a' \mod n$ e $b \equiv b' \mod n$ allora $a+b \equiv a'+b' \mod n$; equivalentemente se $[a]_n = [a']_n$ e $[a]_n = [a']_n$ allora $[a+b]_n = [a'+b']_n$;
2. se $a \equiv a' \mod n$ e $b \equiv b' \mod n$ allora $ab \equiv a'b' \mod n$; equivalentemente se $[a]_n = [a']_n$ e $[a]_n = [a']_n$ allora $[ab]_n = [a'b']_n$;
3. $a \equiv 0 \mod n$ se e solo se n divide a se e solo se $[a]_n = [0]_n$;
4. r è il resto della divisione di a per n se e solo se $0 \leq r < n$ e $[a]_n = [r]_n$;
5. $(a+b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$.
6. $(ab) \bmod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n$.

Congruenze lineari: Guarda gli Appunti di Norberto Gavioli, da pagina 4.

Sia $ax \equiv b \mod n$, allora una soluzione esiste solo se (a, n) divide b.
Si ha $ax - b = hn$ e quindi $b = ax - hn$ è un multiplo di (a, n).
Se x è una soluzione allora è una soluzione anche $x + \dfrac{zn}{(a,n)}$ $\forall z \in \mathbb{Z}$.

Classi di resto

Lemma: Siano a ed n due numeri interi primi tra loro e si supponga che n divida il prodotto ab dove $b \in \mathbb{Z}$; allora n divide b.
Ci sono esattamente n classi di resto modulo n: $[0]_n, [1]_n, \ldots, [n-1]_n$.

Parlando delle classi di resto modulo n, la classe di resto $[r]_n$ di un intero r è data da tutti gli interi che si ottengono da r aggiungendo un multiplo di n: $[r]_n = \{r + kn \mid k \in \mathbb{Z}\} = r + n\mathbb{Z}$.
Ovvero una classe di resto r modulo n è un insieme di numeri interi relativi che divisi per n danno lo stesso resto r.
Ovvero una classe di resto modulo n non è altro che un laterale del sottogruppo $n\mathbb{Z}$ di $\mathbb{Z}$.

Le classi di resto modulo n sono esattamente n.

Dim. del Teorema di Lagrange

Poiché $\sim$ è una relazione di equivalenza, i laterali destri Hg formano esattamente $G : H$ sottoinsiemi disgiunti essendo partizioni, ciascuno dei quali contiene esattamente $|H|$ elementi, poiché $|H| = |Hx| = |xH|$. Ne segue che $|G| = |G : H| \cdot |H|$.