Definizioni e Teoremi di Algebra (senza esempi)

Iniziata lezione 34

Anno accademico 2021/2022

Contents

1 Capitolo 1

Relazione e corrispondenza sono interscambiabili.

1.1 Corrispondenza

Una corrispondenza ρ di X in Y è una terna (ρ, X, Y) dove $\rho \subseteq X \times Y$.

1.2 Relazione in se

Una Relazione di X in sè, è una corrispondenza ρ di X in X. Se $(x, y) \in \rho$ si scrive anche $x\rho y$(notazione infissa), cioè x è in relazione ρ con y.

1.3 Relazione/Corrispondenza inversa

Una corrispondenza ρ di X in Y è la relazione di Y in X denotata con ρ^{-1} data dalla seguente:

$$y\rho^{-1}x \Leftrightarrow x\rho y$$

1.4 Relazione di equivalenza

una relazione su A (cioè un sottoinsieme ρ di AxA) si dice di equivalenza se verifica le tre seguenti proprietà:

Riflessiva: $\forall a \in A, a\rho a$.
Simmetrica: $\forall a, b$ in $A, a\rho b \Rightarrow b\rho a$
Transitiva: $\forall a, b, c \in A$ se $(a\rho b \wedge b\rho c) \Rightarrow a\rho c$

1.5 Relazione banale (di uguaglianza)

Su A $x, y \in A$ $x\rho y \Leftrightarrow x = y$

1.6 Relazione caotica

Su A $x\rho y$ $\forall x, y \in A$

1.7 Classe di equivalenza

Data la relazione ρ in A, si definisce classe di equivalenza modulo ρ di un elemento $a \in A$ l'insieme di tutti gli elementi che sono equivalenti ad a; si denota con $[a]_\rho$.

$$[x]_\rho := \{y \in A : y\rho x\}$$

1.8 Insieme quoziente

Data la relazione di equivalenza ρ su A, si definisce insieme quoziente l'insieme delle classi di equivalenza di ρ dato $x \in A$ si denota con $A/_\rho$.

$$A/_\rho = \{[x]_\rho : x \in A\}$$

Nota: Relazione di equivalenza e partizioni insiemistiche sono sostanzialmente la stessa cosa.

1.9 Partizione insiemistica

Una partizione insiemeistica di A è una famiglia di sottoinsiemi di A non vuoti, tali che ad ogni elemento di A corrisponde un solo sottoinsieme.

$$H = \{A_i : i \in I\}$$

con

$$A_i \subseteq A \; \forall i \in I$$

con

$$i \neq j, \;\; i, j \in I \Leftrightarrow A_i \cap A_j = \emptyset$$

che equivale a dire:

$$\cup_{i \in I} \, A_i = A$$

cioè la famiglia H ricopre A.

1.10 Funzione/Applicazione

$f : S \to T$ è un'applicazione di S in T se (f, S, T) è una corrispondenza di S in T, ovvero $f \subseteq S \times T$ che soddisfa la seguente proprietà:
$\forall x \in S$ $\exists!$ y in T denotato con $y = f(x)$, f è una legge univoca (ben definita).

L'elemento f(x) si chiama **immagine dell'elemento**.

L'immagine di f è un sottoinsieme del codominio T definito da:

$$Im(f) := \{y \in T : \exists \, x \in S, y = f(x)\}$$

Controimmagine di y è il sottoinsieme di S del dominio definito da:

$$f^{-1}(y) := \{x \in S : f(x) = y\} \subseteq S$$

1.11 Iniettiva

f è iniettiva $\Leftrightarrow \forall x, x' \in S : [f(x) = f(x') \Rightarrow x = x']$.
Definizione alternativa: f è iniettiva $\Leftrightarrow \forall x, x' \in S : [f(x) \neq f(x') \Rightarrow x \neq x']$.
f è iniettiva $\Leftrightarrow \forall y \in T \; |f^{-1}| \leq 1$, ovvero per ogni elemento y in T esiste al più un'immagine.

1.12 Suriettiva

f è suriettiva se $\Rightarrow \forall y \in T \ \exists x \in S : f(x) = y$
Definizione alternativa: f è suriettiva $\Leftrightarrow f(S) = Im(S) = T$.
f è suriettiva $\Leftrightarrow \forall y \in T \ |f^{-1}(y)| \geq 1$, ovvero per ogni elemento y in T esiste almeno un'immagine.

1.13 Biunivoca (biiettiva)

se f è sia iniettiva che suriettiva.
f è biiettiva $\Leftrightarrow \forall y \in T \ |f^{-1}(y)| = 1$, ovvero per ogni elemento y in T esiste una sola immagine.

1.14 Funzione caratteristica

E' la funzione che vale 1 se $x \in S$, 0 se $x \notin S$.

1.15 Operazione binaria

Un'operazione binaria su S, è un'applicazione $m : S \times S \to S$; notazione funzionale $(s, s') \mapsto m(s, s')$; notazione infissa sms' o $s * s$.

1.16 Assiomi di Peano

per la costruzione dei naturali $\mathbb{N}$

1. I numeri formano una classe
2. Lo "zero" è un numero
3. Se a è un numero allora il successore a' è un numero
4. Se $a \neq b$ sono due numeri allora $a' \neq b'$
5. Lo "zero" non è successore di nessun numero ($\nexists\, a$ numero tale che $zero = a'$)
6. Assioma di induzione:
   Se S è una classe di numeri tale che:
   - $zero \in S$
   - Se $a \in S$ allora $a' \in S$

   allora ogni naturale è in S.

I naturali sono la più piccola classe che

- Contiene lo zero
- Chiusa rispetto a contenere i successori

1.17 Principio del buon ordinamento di $\mathbb{N}$

Se $S \subseteq \mathbb{N}, S \neq \emptyset$, allora esiste un minimo in S, cioè esiste $m \in S$ tale che se $h \in \mathbb{N}, h < m$ allora $h \notin S$.

1.18 Teor: Divisione con resto su $\mathbb{N}$

Siano $a, b \in \mathbb{N}, b \neq 0$; allora esistono $q, r \in \mathbb{N}$ tali che

- $a = bq + r$
- $0 \leq r < b$

$\forall a, b \in \mathbb{Z}, b \neq 0; \exists$ unici $q, r \in \mathbb{Z}$ con $a = bq + r \wedge 0 \leq r < b$ TODO: Dimostrazione

2 Calcolo combinatorio

2.1 Notazione funzionale

Insieme delle applicazioni da A verso B

$$B^A = \{f : A \to B\}$$

2.2 Fattoriale crescente

$$n^{(m)} := n * (n+1) * ... * (n+m-1)$$

2.3 Fattoriale decrescente

$$n_{(m)} := n * (n-1) * ... * (n-m+1)$$

2.4 Pigenhole principle (principio dei cassetti)

Se ho n oggetti e m cassetti, se $n > m$ e devo disporre tutti gli oggetti nei cassetti allora esiste un cassetto che contiene almeno due oggetti.

2.5 Permutazione

Sia A un insieme. Una biiezione $f : A \to A$ si chiama anche *permutazione* di A.

2.6 Coefficiente binomiale

Prima interpretazione combinatoria: $\binom{n}{i}$ è il coefficiente di $x^i y^{n-i}$ nello sviluppo $(x+y)^n = \sum_{z_i \in \{x,y\}} z_1 ... z_n$, ovvero il numero di stringhe binarie (su x, y)

- lunghe n
- con i occorrenze di x

- con n-i occorrenze di y
- $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$

Seconda interpretazione combinatoria: numero di sottoinsiemi di cardinalità i su un insieme $[n]$ di cardinalità n.

2.7 Formula

$$\binom{n}{i} = \frac{n(n-1) * ... * (n-i+1)}{i!} = \frac{n!}{i!(n-i)!}$$

2.8 Relazione ricorsiva

$$\binom{n}{i} = \binom{n-1}{i-1} + \binom{n-1}{i}$$

Dimostrazioni algebrica e combinatoria.

2.9 Simmetria

$$\binom{n}{i} = \binom{n}{n-i}$$

Il coefficiente binomiale è simmetrico rispetto al centro della riga n-esima $\lfloor \frac{n}{2} \rfloor$ del triangolo rappresentante tutti i coefficienti del coefficiente binomiale.

Dimostrazioni algebrica e combinatoria.

2.10 Relazione d'ordine

Una relazione ρ su X è una relazione d'ordine (o un ordine, o un ordinamento) se valgono per ρ le proprietà:

- (R) $\forall x, x\rho x$
- (AS) $\forall x, y\ (x\rho y \wedge y\rho x) \Rightarrow x = y$
- (T) $\forall x, y, z\ (x\rho y \wedge y\rho z) \Rightarrow x\rho z$

2.11 POSET (Partial order set)

Un insieme munito di una relazione d'ordine si dice parzialmente ordinato.

3 I numeri

3.1 Costruzione di $\mathbb{Z}$ (interi)

Partendo da $\mathbb{N}$: prendiamo su $\mathbb{N} \times \mathbb{N}$ la relazione ρ definita sulle coppie $(n, m) \in \mathbb{N} \times \mathbb{N}$ tale che $(n, m)\rho(n', m') \Leftrightarrow n + m' = m + n'$

3.2 Definizione di $\mathbb{Z}$

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N}/_\rho$$

3.3 Classi su $\mathbb{Z}$

$\overline{(0,0)}$ zero
$\overline{(m,0)}, m > 0$ positivi
$\overline{(0,n)}, n > 0$ negativi

3.4 Sottoinsiemi di $\mathbb{Z}$

$$\mathbb{Z} = \mathbb{Z}^{>0} \cup \{0, 0\} \cup \mathbb{Z}^{<0}$$

3.5 Somma su $\mathbb{Z}$

$$\overline{(n,m)} + \overline{(n',m')} = \overline{(n+n', m+m')}$$

3.6 Prodotto su $\mathbb{Z}$:

$$\overline{(n,m)} \cdot \overline{n', m'} = \overline{(nn' + mm', nm' + mn')}$$

3.7 Proprietà operazioni su $\mathbb{Z}$

$\forall a, b, c \in \mathbb{Z}$ (a, b, c coppie $\overline{(n,m)}$) valgono le seguenti:

1. Associatività: $(a + b) + c = a + (b + c)$
2. Commutatività: $a + b = b + a$
3. Esiste uno *zero* per la somma, cioè un elemento $0 : a + 0 = 0 + a = a$
4. $\forall a \in \mathbb{Z}$ esiste un elemento detto *opposto*, denotato con $-a$, cioè un elemento tale che: $a + (-a) = (-a) + a = 0$.
   $a = \overline{(n,m)}$
   $-a = \overline{(m,n)}$
5. Associatività prodotto: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
6. Commutatività prodotto: $a \cdot b = b \cdot a$

7. Esiste un *elemento neutro* per il prodotto, "1", cioè un numero in $\mathbb{Z}$ tale che:
$$a \cdot 1 = 1 \cdot a = a$$
$$\overline{(n,m)} \cdot \overline{(1,0)} = \overline{(n,m)}$$

8. Distributività del prodotto sulla somma:
$$a \cdot (b+c) = a \cdot b + a \cdot c$$

3.8 Divisibilità

Dati $a, b \in \mathbb{Z}$ si dice che a divide b, e si indica $a|b$, se e solo se $\exists c \in \mathbb{Z}$ tale che $b = a \cdot c$ (ovvero $a|b \Leftrightarrow \exists c \in \mathbb{Z} : b = a \cdot c$).
La divisibilità è una relazione sugli interi:

3.9 Multiplo

Se $a|b$ diremo che b è un multiplo di a.

3.10 Associati

a,b sono associate se $a|b$ e $b|a$
Oss1: in $\mathbb{N}^*$ sono associati $\Leftrightarrow a = b$.
Oss2: in generale, in $\mathbb{Z} \Leftrightarrow a = b$ oppure $a = -b$.

3.11 Unità

In $\mathbb{Z}$ sono +1 e -1.

3.12 Irriducibile

Un elemento $a \in \mathbb{Z},\ a \neq 0$ è irriducibile se $a = b \cdot c \Rightarrow\ b$ oppure c sono unità.

3.13 Primo

Un elemento $a \in \mathbb{Z}$ si dice primo se:
$$a|b \cdot c \Rightarrow a|b \textit{ oppure } b|c$$

3.13.1 Proposizione: in $\mathbb{Z}$, a è primo $\Rightarrow$ a irriducibile

Sia $a = b \cdot c$: usando l'ipotesi che a è primo allora $a|b$ oppure $a|c$.
Se $a|b \Rightarrow \exists\ h : b = a \cdot h \Rightarrow a = a \cdot h \cdot c \Rightarrow h \cdot c = 1 \Rightarrow c = \pm 1$
Allora $a = b \cdot (+1)$ oppure $a = b \cdot (-1)$, a è irriducibile.

3.13.2 Proposizione: in $\mathbb{Z}$ a irriducibile⇒a primo

Ipotesi: a irriducibile
Tesi: a primo Supponiamo che $a|bc \Leftrightarrow \exists h \in \mathbb{Z} : bc = ah$,
voglio mostrare che $a|b$ oppure $a|c$ ovvero che se $a \nmid b$ allora $a|c$.
Ora a irriducibile, i suoi divisori sono $a, -a, 1, -1$. $a \nmid b$ allora anche $-a \nmid b \Rightarrow$i divisori comuni tra a e b sono $1, -1 \rightarrow MCD(a, b) = 1$.

$$\exists(\text{id. Bézout})\exists\ h, k \in \mathbb{Z}$$

$$1 = ah + bk$$

moltiplicando per c

$$c = cah + cbk = a(ck + k) \quad [cb = a]$$

quindi $a|c$.

3.14 Massimo comune divisore

Dati a,b non entrambi nulli, un elemento $d \in \mathbb{Z}$ si chiama massimo comune divisore tra a e b un numero tale che:

- $d|a \wedge d|b$
- Se $c|a \wedge c|b$, allora $c|d$: d è il massimo tra i divisori comuni.

Chiamiamo massimo comune divisore l'unico positivo che soddisfa le due proprietà.

3.14.1 Teor: Esistenza del MCD tra due numeri

$\forall a, b \in \mathbb{Z}$ non entrambi nulli, esiste un numero $d \in \mathbb{N}^*$ tale che $d = MCD(a, b)$
Il massimo comune divisore si esprime come una combinazione lineare tra a e b, ovvero esistono $s, t \in \mathbb{Z}$ tali che $d = s \cdot a + t \cdot b$ (*identità di Bézout*).

Dimostrazione:
Sia $S = \{xa + yb : x, y \in \mathbb{Z}, xa + yb > 0\}$

1. $S \subseteq \mathbb{N}$
2. $S \neq \emptyset$

a e b sono non entrambi nulli, quindi almeno uno dei due è $\neq 0$. Sia esso a.
Se $a > 0$ allora $1 \cdot a + 0 \cdot b = a > 0$ Se $a < 0$ allora $(-1) \cdot a + 0 \cdot b = a > 0$
TODO: completare dimostrazione

Dimostrazione che $d|a$ e $d|b$:
Dividiamo a per d (divisione col resto): $\exists\ q, r$ con $a = dq + r,\ 0 \leq r < d$
Se $r = 0$ allora $d|a$
Se $r \neq 0$ allora $0 < r < d$
$r = a - dq$; dato che $d \in S \Rightarrow d = x_0a + y_0b$ allora

$r = a - q(x_0 a + y_0 b) = a - qx_0 a + qy_0 b = a(1 - qx_0) - (qy_0)b$
Quindi $r \in S$ perchè è una combinazione lineare > 0 ma $r < d$, però d è il minimo di $S \Rightarrow$Assurdo.

Dimostrazione se $d'|a$ e $d'|b$ allora $d'|d$:
Poichè $d'|a$ e $d'|b$ si ha che

$$\exists h : a = d' \cdot h, \exists k : b = d' \cdot k$$

Ora

$$d = x_0 a + y_0 b$$
$$= x_0(d'h) + y_0(d'k) =$$
$$= d'(x_0 h + y_0 h) \Rightarrow d'|d$$

3.14.2 Prop: se $c|a$ e $c|b$ allora c divide ogni combinazione lineare di a e b

$$a = ch$$
$$b = ck$$
$$\Rightarrow xa + yb = xch + yck$$
$$= c(xh + yk) \Rightarrow \in \mathbb{Z}$$
$$\Rightarrow c|xa + yb$$

3.15 Proposizione

$$1 = at + bs \Rightarrow MCD(a, b) = 1$$

3.15.1 Lemma MCD(m,m+1)=1

Sia $m \in \mathbb{N},\ m \geq 1$ allora $MCD(m, m + 1) = 1$.

Dimostrazione:

$$m + 1 - m = 1 \Rightarrow 1(m + 1) + (-1)m = 1$$

Potendo scrivere *1* come combinazione lineare di *m* e *m+1*, *m* e *m+1* sono primi tra loro.

3.16 Algoritmo di Euclide

3.16.1 Lemma1: L'algoritmo termina

La successione dei resti è un numero $0 \leq ... < r_2 < r_1 < b$.

3.16.2 Lemma2: Se $a = bq + r$ $MCD(a,b) = MCD(b,r)$

TODO: scrivere dimostrazione

3.16.3 Corollario: $MCD(a,b) = MCD(r_n, 0) = r_n 1$

Per il lemma 2 $MCD(a,b) = MCD(b,r_1) = MCD(r_1,r_2) = ... = MCD(r_{n-1},r_n) = MCD(r_n, 0)$

3.16.4 Lemma3

Se $x \in \mathbb{N}^*$ allora $MCD(x,0) = x$

3.17 Coprimi

a,b non entrambi nulli, *a* e *b* si dicono coprimi (o *primi fra loro*) se *MCD(a,b)=1.*

3.17.1 Osservazione1

Se a e b sono primi fra loro, allora

$$\exists\, x, y \in \mathbb{Z} : 1 = xa + yb$$

3.17.2 Osservazione 2

Se

$$d = MCD(a,b) \Rightarrow \exists\, x, y : d = ax + by$$

3.17.3 Proposizione 1

Se $\exists\, x_0, y_0$ con $1 = ax_0 + by_0$ allora *a,b* sono primi tra loro.

3.17.4 Proposizione 2

Se a e b sono coprimi e dividono un terzo numero c, allora $ab|c$.

3.18 Equazione diofantea

Equazione con una o più incognite sugli interi di cui si cercano le soluzioni intere.
Sono del tipo:

$$ax + by = c$$

3.18.1 Teor: Soluzione equazione diofantea

L'equazione diofante lineare in x e y $ax + by = c \quad a, b, c \in \mathbb{Z}$ possiede soluzioni intere $(x, y) \in \mathbb{Z}^2 \Leftrightarrow d = MCD(a, b)|c$
(Dim$\Rightarrow$) La condizione $MCD(a, b)|c$ è necessaria.
Ipotesi: esiste una soluzione di $x^2 + y^2 = z^2$
Tesi: $d|$termine noto, $d = MCD(a, b) : d|a$ e $d|b \Rightarrow d|$ ogni combinazione lineare di *a,b*.
Se x_0, y_0 sono una soluzione, allora $ax_0 + by_0 = c \Rightarrow d|c = ax_0 + by_0$

(Dim$\Leftarrow$) La condizione è sufficiente.
Ipotesi $MCD(a, b) = ah + bk$, per opportuni $h, k \in \mathbb{Z}$

3.19 Teorema fondamentale dell'aritmetica

$\forall n > 1, n \in \mathbb{N}, \exists\ p_1, ..., p_j \in \mathbb{N}$ (irriducibili) $\exists h_1, ..., h_j \geq 1$ tali che:

- $n = p_1^{h_1} ... p_j^{h_j} \quad p_1, ...p_j$ distinti
- la fattorizzazione di $n = p_1^{h_1} ... p_j^{h_j} \quad p_1, ...p_j$ è unica a meno di riordinare i fattori

3.19.1 Osservazione 1

j può essere 1, cioè potrebbe esserci un solo irriducibile nella fattorizzazione di n, anche h possono essere 1. Se n è irriducibile $\Rightarrow n = n$ è la fattorizzazione in irriducibili di n.

3.19.2 Osservazione 2

1 non è considerato irriducibile perché si perderebbe l'unicità della scrittura in irriducibili.

3.19.3 Dimostrazione esistenza

Con principio di induzione in forma forte.
Base: *n=2*, 2 è irriducibile.
Per **oss1** $2 = 2^1$ è la fattorizzazione in primi in irriducibili di 2
Ipotesi induttiva: ogni $2 \leq a < n \quad (2 \leq a \leq n-1)$ è fattorizzabile in irriducibili: $\exists\ \alpha_1 ... \alpha_t \alpha_i \leq 1$ e $q_1, ...q_t$ irriducibili con $a = q_1^{\alpha_1} ... q_t^{\alpha_t}$
Passo induttivo: provare che n sia prodotto di irriducibili

Primo caso: n irriducibile $\rightarrow$ fatto, per *oss.1*

Secondo caso: n riducibile: $\exists\ b, c \in \mathbb{Z}, 1 \neq b, c \neq n$ (divisori propri) con

$n = bc \Rightarrow 2 \leq b, c < n$.
Allora per b e c vale l'ipotesi induttiva e quindi

$$b = q_1^{\alpha_1}...q_t^{\alpha_t} \quad c = x_1^{\beta_1}...x_s^{\beta_s}$$

$$n = bc = q_1^{\alpha_1}...q_t^{\alpha_t} x_1^{\beta_1}...x_s^{\beta_s}$$

3.20 Dimostrazione unicità

Per induzione su m, con m è la lunghezza minima di una fattorizzazione per n.
m: minimo numero di irriducibili di una fattorizzazione di n
Base: $m = 1 \Rightarrow n = n$ è primo.
Se per assurdo $n = q_1...q_s,\ s \geq 2$ allora $n|q_1$ o $n|q_2...q_s$.
Prendiamo $n|q_1$, anche q_1 è primo $\Rightarrow n = q_1$; semplificando da entrambe le parti $\Rightarrow 1 = q_2....q_s$ che porterebbe ad un assurdo perché $1 = 1$.
Quindi $n = q_1$ ed è l'unica fattorizzazione.

Ipotesi induttiva: se il minimo numero di primi in una fattorizzazione di n è $m-1$, allora la fattorizzazione è unica a meno dell'ordine.

Passo induttivo: m è il minimo di una fattorizzazione di n.

3.21 Teor. Euclide - Esistenza infiniti primi

L'insieme $P = \{p \in \mathbb{N} : \text{p è primo}\}$ è infinito.
Dimostrazione: Supponiamo che P sia finito, cioè $P = \{p_1, ..., p_n\}$.
Sia $m = p_1, ...p_n$ il prodotto di tutti i primi.
Considero $m+1$: per il teorema fondamentale dell'aritmetica $m+1 = p_1^{k_1}...p_n^{k_n}$, $k_1, ..., k_n \geq 0$ almeno uno degli esponenti > 0.
Per il lemma su MCD di un numero ed il suo successivo m e *m+1* sono coprimi.
Sia j tale che $k_j > 0$, cioè $p_j^{k_k}|m{+}1$; vale anche $p_j|m$ allora $p_j|MCD(m, m{+}1) = 1$ che è un assurdo.

4 Congruenze

4.1 Congruenza modulo n

La congruenza modulo n (n fissato) è una relazione di equivalenza definita su $\mathbb{Z}$.

$x \equiv y(mod\ n) \Leftrightarrow x - y$ multiplo di $n \Leftrightarrow n|x - y$

4.2 Proposizione

La congruenza *(mod n)* è una relazione di equivalenza.
Dimostrazione:

(R)

$$\forall x \in \mathbb{Z} : x \equiv x(mod\ n) \Leftrightarrow n|(x - x)$$

Vera perché $0 = 0 \cdot n$.

(S)

$$\forall x, y \in \mathbb{Z} : x \equiv y(mod\ n) \Rightarrow y \equiv x(mod\ n)$$

So che $n|x - y \Leftrightarrow x - y = nh$ per qualche $h \in \mathbb{Z}$.

Moltiplicando per *-1*: $y - x = -nh = n(-h)$ quindi $n|y - x \Rightarrow y \equiv x(mod\ n)$

(T)

$$x \equiv y(mod\ n) \wedge y \equiv z(mod\ n) \Rightarrow x \equiv z(mod\ n)$$

$(x - y) = nh_1 \wedge (y - z) = nh_2$
$(x-z) = (x-y)-(y-z) = nh_1-nh_2 = n(h_1-h_2)$ quindi $n|x-z \Rightarrow x \equiv z(mod\ n)$

4.3 Quoziente

Il quoziente della congruenza *(mod n)* si denota come $\mathbb{Z}_{/\equiv(mod\ n)} = \{[x]_n : x \in \mathbb{Z}\}$.
Il quoziente $\mathbb{Z}_n$ si chiama anche **interi modulo n**.

4.4 Proposizione

Dati $x, y \in \mathbb{Z}$ si ha: $x \equiv y(mod\ n) \Leftrightarrow$ il resto delle divisioni di x e di y per n è lo stesso.
Dimostrazione $\Rightarrow$**(se** $x \equiv_n y$ **hanno lo stesso resto** $x - y = nh$ (per qualche h)
$x = nh + y$
Dividendo y per n: $\exists! q, r \in \mathbb{Z} : y = nq + r,\ 0 \leq r < n$.
Scambiando in x: $x = nh + nq + r = n(h + q) + r$, x ed y hanno quindi lo stesso resto.

4.5 Osservazione

Sia $x = nq + r,\ 0 \leq r < n$ la divisione con resto di x per n.
Allora
$$[x]_n = [r]_n \Leftrightarrow x \equiv r(mod\ n) \Leftrightarrow x - r = nq$$
Quindi
$$n|x - r$$

4.6 Proposizione somma

La somma classi resto in $\mathbb{Z}_n$, definita da: $\overline{x} + \overline{y} := \overline{x + y}$, è ben posta, ovvero non dipende dalla scelta dei rappresentanti.
Dimostrazione Siano $x' \in \overline{x}$, cioè $\overline{x'} = \overline{x}$ e $y' \in \overline{y}$ cioè $\overline{y'} = \overline{y}$, allora

$$x' \equiv x(mod\ n) \Leftrightarrow x' = x + kn$$
$$y' \equiv y(mod\ n) \Leftrightarrow y' = y + hn$$

Da verificare: $\overline{x' + y'} = \overline{x + y} \Leftrightarrow x' + y' = x + y + tn$
Quindi:
$$x' + y' = x + kn + y + hn$$
$$= x + y + kn + hn$$
$$= x + y + (k + h)n\ \ [(k + h) = t]$$

4.7 Dimostrazione prodotto

$$x' \cdot y' = (x + kn)(y + hn)$$
$$= xy + xhn + kny + khn^2$$
$$xy + n(xh + ky + khn), \quad [(xh + ky + khn) = t]$$

4.8 Proposizione

$a \in \mathbb{Z}, \overline{a}$ invertibile in $\mathbb{Z}_n \Leftrightarrow MCD(a, n) = 1$
Dim $\Rightarrow$
Ipotesi: $\overline{a} \in \mathbb{Z}$ invertibile

Tesi: *(a,n)=1*

Esiste $b \in \mathbb{Z} : \overline{a} \cdot \overline{b} = 1$
$$\Leftrightarrow ab \equiv 1(mod\ n)$$
$$\Leftrightarrow n|1 - ab$$
$$\Leftrightarrow 1 - ab = nk$$
$$\Leftrightarrow 1 = ab + nk$$

$$\Rightarrow MCD(a,n)=1$$

Dim $\Leftarrow$
Ipotesi: $MCD(a,n)=1$

Tesi: $\overline{a}$ è invertibile

Se $MCD(a,n)=1$ allora esistono $h,k\in\mathbb{Z}:$

$$1=ah+nk \quad \in\mathbb{Z}$$
$$\overline{1}=\overline{ah+nk}$$
$$\overline{1}=\overline{a}\overline{h}+\overline{n}\overline{k} \quad \in\mathbb{Z}$$
$$\overline{n}\overline{k}=\overline{0}\overline{k}$$
$$\overline{1}=\overline{a}\overline{h}\Rightarrow\overline{h}=(\overline{a})^{-1}$$

4.9 Classi resto invertibili

$$\cup(\mathbb{Z}_n):=\{a\in\mathbb{Z}_n:\overline{a}\ invertibile\}\subseteq\mathbb{Z}_n$$
$$\cup(\mathbb{Z}_n)=\{\overline{a}:MCD(a,n)=1\}$$

4.10 Teorema Uguaglianza sbagliata

Se p è primo allora $\forall x,y\in\mathbb{Z}$ vale:

$$(x+y)^p\equiv x^p+y^p(mod\ p)$$
$$(\overline{x}+\overline{y})^p=\overline{x}^p+\overline{y}^p(mod\ p)$$

Dimostrazione:$(x+y)^p=\sum_{i=0}^{p}\binom{p}{i}x^iy^{p-i}$

$$\binom{p}{0}=1=\binom{p}{p}$$
$$\binom{p}{0}x^0y^p=1y^p$$
$$\binom{p}{p}x^py^0=1x^p$$

Considerare con $0<i<p$ il coefficiente binomiale è:

$$\binom{p}{i}=\frac{p(p-1)...(p-i+1)}{i(i-1)...2\cdot1}\in\mathbb{N}$$
$$p(\frac{(p-1)...(p-i+1)}{i!})\Rightarrow p|\binom{p}{i}\forall i=2,...,p-1$$
$$\Rightarrow\binom{p}{i}\equiv0(mod\ p)$$

4.10.1 Grande teorema di Fermat

$x^n + y^n = z^n, n \geq 3$ non ha soluzioni intere.

4.10.2 Piccolo teorema di Fermat

$\forall a \in \mathbb{Z}, \forall p(mod)$ primo si ha che: $a^p \equiv a(mod\ p)$ in $\mathbb{Z}_{|}$, p primo vale $\overline{a}^p = \overline{a}$.

Dimostrazione per $a \in \mathbb{N}$
Per induzione su a

Base:

$$a = 0$$
$$0^p \equiv^? 0(mod\ p)$$
$$0^p = 0 \in \mathbb{Z} \Rightarrow 0^p \equiv (mod\ p)$$

Ipotesi induttiva: supponiamo vera per a l'affermazione $a^p \equiv a(mod\ p)$

Passo induttivo: verifichiamo per $(a + 1)$.

$$(a + 1)^p \equiv a^p + 1^p \equiv a + 1$$

$a^p \to a$ e $1^p \to 1$ per ipotesi induttiva.

Se $a < 0$ è ancora vero?
Se $a < 0$ allora $-a > 0$, cioè $(-a)^p \equiv -a(mod\ p)$. Ora:

$$0 = a - a$$
$$0^p = (a - a)^p$$
$$0^p \equiv (a - a)^p \equiv a^p + (-a)^p$$
$$\equiv a^p - a \equiv 0 \cdot (mod\ p) \Leftrightarrow a^p \equiv a(mod\ p)$$

4.11 Teorema Eulero-Fermat

Se $(a, p) = 1$ cioè se $\overline{a} \neq \overline{0}$ in $\mathbb{Z}_p$ allora

$$a^{p-1} \equiv 1(mod\ p)$$

Dimostrazione: se $(a, p) = 1$ allora esiste l'inverso moltiplicativo di $\overline{a}$ in $\mathbb{Z}_p$.
So che

$$a^p \equiv a(mod\ p)$$
$$(\overline{a}^p) \equiv \overline{a}(mod\ p)$$
$$\Rightarrow moltiplicando\ per\ l'inverso \Rightarrow \overline{a}^{p-1} = \overline{1}\ in\ \mathbb{Z}_p$$
$$\Leftrightarrow a^{p-1} \equiv 1(mod\ p)$$

4.12 Corollario

Se $(a, p) = 1$ e se p primo allora $\overline{a}^{p-2}$ è l'inverso moltiplicativo di $\overline{a}$ in $\mathbb{Z}_p$

Dimostrazione: l'inverso di $\overline{a}$ è $\overline{x}$ con $\overline{a} \cdot \overline{x} = \overline{2}$, ma

$$\overline{a} \cdot \overline{a}^{p-2} = \overline{a}^{p-1} = \overline{1}$$

per il *teorema di Eulero-Fermat*.

5 Polinomi a coefficienti reali in 1 indeterminata

5.1 Descrizione

$$\mathbb{R}[x] := \{p(x) = a_0 + a_1x + a_2x^2 + ... + a_kx^k : a_i \in \mathbb{R}, i = 0, ..., k, k \in \mathbb{N}\}$$

5.2 Somma di polinomi

Dati

$$p(x) = a_0 + a_1x + a_2x^2 + ... + a_kx^k$$
$$q(x) = b_0 + b_1x + b_2x^2 + ... + b_kx^k$$

con $k \leq h$

$$p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x + ... + (a_k + b_k)x^k + b_{k+1}x^{k+1} + ... + b_hx^h$$

5.3 Rappresentazione come successioni

Con esempio:

$$p(x) = 1 + 3x - 4x^3 \leftrightarrow (1, 3, 0, -4, 0, 0, ...)$$

5.3.1 Somma di polinomi

$$p(x) = (a_0, a_1, a_2, ...)$$
$$q(x) = (b_0, b_1, b_2, ...)$$
$$p(x) + q(x) = (a_0 + b_0, a_1 + b_1, ..., a_n + b_n, ...)$$

a_i, b_i sono i coefficienti di x^i nel polinomio che rappresentano.

5.4 Teorema: $(\mathbb{R}[x], +)$ è un gruppo (commutativo)

Dimostrazione:

- $\mathbb{R}[x]$ è non vuoto
- La somma è associativa

  $$(\underline{a} + \underline{b}) + \underline{c} = (...(a_n + b_n) + c_n...) = (...a_n + (b_n + c_n)...) = \underline{a} + (\underline{b} + \underline{c})$$

- $0 \in \mathbb{R}$ è l'elemento neturo di $\mathbb{R}[x]$

  $$0 = 0 + 0x + 0x^2 + ... \rightarrow (0, 0, 0, ...)$$

- Ogni polinomio ha il suo opposto: se

  $$p(x) = a_0 + a_1x + ... + a_kx^k$$

  allora l'opposto di $p(x)$ è

  $$-p(x) = -a_0 - a_1x - ... - a_kx^k$$

5.5 Prodotto di polinomi

$$p(x) = a_0 + a_1x + ... + a_kx^k \leftrightarrow (a_0, a_1, ...)$$
$$q(x) = b_0 + b_1x + ... + b_kx^k \leftrightarrow (b_0, b_1, ...)$$
$$p(x) \cdot q(x) = c_0 + c_1x + ...c_rx^r \leftrightarrow (c_0, c_1, ...)$$

$$c_0 + c_1x + ...c_rx^r = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2+$$
$$+(a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)x^3 + ...$$

La successione dei coefficienti di $p(x) \cdot q(x)$ è data da:

$$c_n = \sum_{i=0}^{n} a_ib_{n-i} = \sum_{i+j=n} a_ib_j$$

5.6 Teorema $(\mathbb{R}, +, \cdot)$ è un anello

$(\mathbb{R}, +, \cdot)$ è un anello commutativo, unitario con unità del prodotto uguale a 1 ed è un dominio di integrità. *non dimostrato*

5.7 Grado del prodotto

Se il grado di $p(x) = k$ èd il grado di $q(x) = h$ il grado del prodotto $p(x)q(x) = k + h$

5.8 Fatti importanti

- in $\mathbb{R}[x]$ si può fare la "divisione col resto":

  $$\forall a(x), b(x) \in \mathbb{R},\ b(x) \neq 0$$
  $$\exists!\ q(x), r(x) \in \mathbb{R} :$$

  1. $a(x) = b(x) \cdot q(x) + r(x)$
  2. il grado di $r(x) <$ grado $b(x)$

- Conseguenza della divisione col resto:

  $$MCD(m(x), n(x))$$
  $$m(x) = n(x) \cdot q_1(x) + r_1(x)$$
  $$n(x) = r_1(x) \cdot q_2(x) + r_2(x)$$
  $$...$$

  Termina quando il resto è un polinomio di grado 0.

6 Strutture algebriche

6.1 Gruppo

Un insieme S non vuoto, munito di una operazione

$$m : S \times S \to S$$

$$(a, b) \mapsto m(a, b) = a * b \ \ (notazione\ infissa)$$

che verifica i punti 1, 3, 4 si chiama *gruppo*$(S, *)$.
L'operazione su S è dunque:

- associativa
- con elemento neutro e: $\forall x, x * e = e * x = x$
- per ogni elemento x esiste un inverso rispetto al prodotto $*$ cioè un elemento y tale che $x * y = y * x = e$, che si denota x^{-1}

6.2 Gruppo commutativo (abeliano)

Se il gruppo $(S, *)$ soddisfa anche la proprietà 2 (quindi associatività, elemento neutro, opposto, +commutatività).

6.3 Anello

Un anello è una terna $(A, +, \cdot)$ con:

- A insieme non vuoto
- $+ \cdot$ due operazioni binarie, associative
- $(A, +)$ è un gruppo abeliano
- Distributività: $\forall a, b, c \in A,\ a \cdot (b + c) = a \cdot b + a \cdot c$

6.3.1 Anello commutativo

Se un anello $(A, +, \cdot)$ il prodotto è commutativo, cioè se $\forall a, b \in A,\ a \cdot b = b \cdot a$.

6.3.2 Anello unitario

Se esiste un elemento di A, che si denota con 1_A, tale che $a \cdot 1_A = 1_A \cdot a = a$.

6.3.3 Divisore dello zero

Un elemento $a \in A,\ a \neq 0_A$ di un anello di dice divisore dello zero se esiste $b \in A, b \neq 0$ con $a \cdot b = 0_A$.

6.3.4 Dominio di integrità

Se $(A, +, \cdot)$ è privo di divisori dello zero.

6.3.5 Legge di annullamento del prodotto

Se in un dominio di integrità $a \cdot b = 0_A$ allora $a = 0_A$ oppure $b = 0_A$.

6.4 Campo

Un campo è una terna $(K, +, \cdot)$ con K insieme non vuoto e 2 operazioni.

- $(K, +, \cdot)$ anello commutativo unitario
- Detto 0_k l'elemento neutro della somma e denotato con $K^* = K \setminus \{0_k\}$, deve valere che $\forall x \in K^* : x \cdot x^{-1} = 1_k$

Quindi campo $\Leftrightarrow$ anello commutativo unitario con in più $K \setminus \{0_k\} = (K^*, \cdot)$ gruppo.

6.5 Semigruppo

Sia X un insieme non vuoto.
$*$:

$$X \ * \ X \to Z$$

$$(a.b) \mapsto a * b$$

una operazione binaria associativa: $\forall a, b, c \in X : a + (b + c) = (a + b) + c$
Un insieme X, munito di una operazione associativa si chiama **semigruppo**.

6.5.1 Monoide

Se $(X, +)$ è un semigruppo ed inoltre esiste un elemento 1_X tale che $a + 1_X = 1_X * a = a$ (1_X elemento neutro dell'operazione $*$), allora $(X, +)$ si chiama **monoide**.

6.6 Elenco gruppi

$(A^*, \cdot)$ è un monoide non commutativo.
$(\mathbb{N}, +)$ (commutativo) monoide (0 el. neutro) ma non è un gruppo.
$(\mathbb{Z}, +)$ gruppo commutativo (0 el. neutro).
$(\mathbb{Q}, +)$ gruppo commutativo (0 el. neutro); $\frac{p}{a} \to \textit{opposto} \ -\frac{p}{q}$.
$(\mathbb{N}^*, \cdot)$ monoide, non è un gruppo.
$(\mathbb{Z}^*, \cdot)$ monoide, non è un gruppo.
$(\mathbb{Q}, \cdot)$ non è un gruppo, 0 non ha inverso.
$(\mathbb{Q}^*, \cdot)$ gruppo.
$(\mathbb{R}, +)$ gruppo.
$(\mathbb{R}^*, \cdot)$ monoide, gruppo.

$(\mathbb{Z}_n, +)$ gruppo finito commutativo; el. neutro $\overline{0}$.
$(\mathbb{Z}_n, \cdot)$ monoide, semigruppo (non è un gruppo $\overline{0}$ non è invertibile).
$(\cup(\mathbb{Z}_n), \cdot)$ gruppo, el. neutro $\overline{1} = \{\overline{a} : (a, n) = 1\}$ (el. invertibili).

6.7 Gruppo simmetrico

6.7.1 Permutazione

$f : [n] \to [n]$ si chiama permutazione di n *elementi* se f è biiettiva.

6.7.2 S_n

$$\begin{aligned} S_n &:= \{\sigma : [n] \to [n] : \sigma\ e'\ biiettiva\} \\ &= \{\sigma : \sigma\ e'\ una\ biiezione\} \end{aligned}$$

6.7.3 Proposizione

$$|S_n| = n!$$

6.7.4 Proposizione

$(S_n, \cdot)$ l'insieme delle permutazioni di n elementi con il prodotto di composizione funzionale è un gruppo di cardinalità *n!* non commutativo.
Dimostrazione

- S_n non vuoto, $n \geq 1$
- Esiste un elemento neutro rispetto al prodotto $\cdot$, la permutazione identica: $\sigma \circ id = id \circ \sigma = \sigma$.
- Prodotto associativo $\forall \sigma, \tau, \rho \in S_n$ $(\sigma \circ \tau) \circ \rho(i) = \sigma \circ (\tau \circ \rho)(i) = \sigma(\tau(\rho(i)))$
- $\forall \sigma \in S_n$ esiste un elemento σ^{-1} tale che $\sigma \circ \sigma^{-1} = id$.

6.7.5 3^a notazione: Permutazione come prodotto di cicli disgiunti

S_n: Definire una relazione di equivalenza su $[n]$ associata a $\sigma \in S_n$.

$$x, y \in [n]$$

$$x \equiv_\sigma y \Leftrightarrow \exists i : y = \sigma^i(x)$$

Si osservi che $\sigma \in S_n$, allora la potenza *i-esima* di σ, con $i \in \mathbb{N}$ è la permutazione $\sigma^i = \sigma \circ ... \circ \sigma$ per i volte.

6.7.6 Orbita

L'orbita di $x \in [n]$ è la classe di equivalenza di x nella relazione $\equiv_\sigma$.

$$O_\sigma(x) = \{y \in [n]\ \exists i\ con\ y = \sigma^i(x)\}$$

6.7.7 Proposizione

Se τ_1 e τ_2 hanno cicli disgiunti $\tau_1 \circ \tau_2 = \tau_2 \circ \tau_1$

6.7.8 Permutazione ciclica

Chiamo ciclica una permutazione di S_n) in cui nella rappresentazione in cicli disgiunti ha al più un solo ciclo di lunghezza> 1

6.7.9 Teorema prodotto di scambi

Ogni permutazione si può scrivere come prodotto di scambi

Dimostrazione 1: Se la permutazione ha un solo ciclo $\sigma = (a_1, a_2, ..., a_k) =$ un k-ciclo $= (a_1, a_k)(a_1, a_{k-1})...(a_1, a_3)(a_1, a_2) = (a_1, a_2, a_3, ..., a_k)$
Dimostrazione 2: Se ho un σ qualunque, allora

$$\sigma = C_1 \cdot C_2 \cdot ... \cdot C_k$$

dove C_i è un ciclo (nella decomposizione in cicli disgiunti)

$$C_1 = (a_1, ..., a_r) = (a_1, a_r)(a_1, a_{r-1})...(a_1, a_2)$$

$$C_2 = (b_1, ..., b_j) = (b_1, b_j)(b_1, b_{j-1})...(b_1, b_2)$$

$$...$$

$$\sigma = (a_1, a_r)(a_1, a_{r-1})...(a_1, a_2)\ (b_1, b_j)(b_1, b_{j-1})...(b_1, b_2)$$

6.7.10 Teorema parità

Il numero di scambi usati in diverse fattorizzazioni di una permutazione ha sempre la stessa parità.

6.7.11 Pari, dispari

Una permutazione è pari se il numero di scambi (in una sua fattorizzazione in scambi) è pari, dispari altrimenti.

6.7.12 Gruppo alterno

Le premutazioni pari si chiamano *gruppo alterno*.

6.7.13 Segno

Data σ in S_n, il segno di σ è $\varepsilon(\sigma) = (-1)^{parita'\ di\ (\sigma)}$

6.8 Classi coniugate in S_n

6.8.1 Definizione

Dato G gruppo rispetto ad un'operazione $\cdot$, un elemento x' si dice coniugato con $x \Leftrightarrow$

$$\exists y \in G \; con \; : x' = yxy^{-1}$$

In S_n σ, σ' sono coniugate $\Leftrightarrow$

$$\exists \tau \in S_n : \sigma' = \tau\sigma\tau^{-1}$$

(si dice che σ' è coniugato a σ tramite τ)
TODO: controllare correttezza definizione

6.8.2 Proposizione

Due permutazioni $\sigma, \sigma' \in S_n$ sono coniugate $\Leftrightarrow$ hanno la stessa struttura ciclica.

6.9 Definizione multinsieme

Una partizione λ di un intero n è un multinsieme di naturali ≥ 1 la cui somma da n.

6.10 Gruppi finiti

6.10.1 Proprietà 1

Dato $(G, \cdot)$ gruppo e $x, y \in G$ allora $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$ (l'inverso del prodotto è il prodotto degli inversi in ordine inverso).

Dimostrazione: $(xy)^{-1} =^? e_G$ (el. neutro del gruppo).
Ora

$$(x \cdot y)^{-1} \cdot (y^{-1} \cdot x^{-1}) =$$
$$x \cdot (y \cdot y^{-1}) \cdot x^{-1} =$$
$$x \cdot e_G \cdot x^{-1} =$$
$$x \cdot x^{-1} =$$
$$e_G$$

6.10.2 Proprietà 2

In un gruppo vale sempre la cancellazione:

$$ax = bx \Leftrightarrow a = b$$

Dimostrazione: $\exists x^{-1}$: Se $ax = bx$ e moltiplico per x^{-1}

$$axx^{-1} = bxx^{-1}$$

$$a \cdot e = b \cdot e$$

$$a = b$$

Conseguenza: Su una riga (qualunque) della tavola moltiplicativa del gruppo ci sono una e una sola volta tutti gli elementi del gruppo.

6.11 Sottogruppi

6.11.1 Definizione

Un sottogruppo S di $(G, \cdot)$ è:

- Un sottoinsieme non vuoto di $S \subseteq G$
- S, con la stessa operazione di G è un gruppo

6.11.2 Criteri di verifica

Per verificare che S sia un sottogruppo di G;

- Associatività: *"gratis"* : $S \subseteq G$ e il prodotto in G è associativo.

1. $\forall a, b \in S : a \cdot b \in S$ ovvero $S \times S \to S$
2. $e_G \in S$
3. $\forall a \in S \subseteq G$, $a^{-1} \in S$

6.11.3 Notazione

$$(S, \cdot) \leq (G, \cdot)$$

altrimenti

$$S \leq G$$

6.11.4 Proposizione

S non vuoto e $S \subseteq (G, \cdot)$ è un sottogruppo di G se e solo se

$$\forall\, a, b \in S : a \cdot b^{-1} \in S \quad (*)$$

Dimostrazione
Ipotesi: $\forall a, b : a \cdot b^{-1} \in S$
Tesi: valgono 1, 2, 3 dei criteri di verifica.

Dimostrazione 2:
$S \neq \emptyset : \exists a_0 \in S$ applico $(*)$ ad a_0, a_0:

$$a_0 \cdot a_0^{-1} = e_G \ \in S$$

è quindi l'elemento neutro.

Dimostrazione 3:
$\forall a \in S : a^{-1} \in S$? Per 2. $e_G \in S, a \in S$, applico $(*)$

$$e_G \cdot a^{-1} = a^{-1} \ \in S$$

Dimostrazione 1:
Dati $a, b \in S$, $a \cdot b \in S$? Per la 3 $b^{-1} \in S$.
Dati a, b^{-1} per $(*)$

$$a \cdot (b^{-1})^{-1} = a \cdot b \ \in S$$

6.12 Proposizione: intersezione di sottogruppi

Sia $(G, \cdot)$ un gruppo e $H \leq G, K \leq G$ due sottogruppi. Allora:

$$H \cap K \leq G$$

L'intersezione di sottogruppi di G è un sottogruppo di G

Dimostrazione:

1. $1_G \in H \cap K$?
   Poiche H e K sono sottogruppi $1_G \in H, K$ e quindi $1_G \in H \cap K$
2. Siano $x, y \in H \cap K$: verifico che $x \cdot y \in H \cap K$.
   $x \in H$ *e* $x \in K$; $y \in H$ *e* $y \in K$ allora:

   $$xy \in H;\ xy \in K \Rightarrow xy \in H \cap K$$

3. Se $x \in H \cap K \Rightarrow x^{-1} \in H \cap K$?
   La dimostrazione è simila a quella del punto precendente

6.13 Proposizione 1

$$H_1, H_2, ...H_t \leq G \Rightarrow H_1 \cap H_2 \cap ... \cap H_t \leq G$$

6.14 Proposizione 2

Siano $S, T \leq G$:

$$S \cup T \leq G \Leftrightarrow S \cup T = T \vee S \cup T = S$$

7 Sottogruppo generato

7.1 Definizione

Siano G un gruppo e $X \subseteq G$, si definisce sotto gruppo generato di X il più piccolo sottogruppo di G che contenga X

7.2 Notazione

$$\langle X \rangle := \bigcap_{X \subseteq H \leq G} H$$

7.3 Proposizione

Se $X = \{x_, x_2 ...\} \subseteq G \neq 0$ allora:

$$\langle X \rangle = \{t_1, t_2, ..., t_r : t_i \in X \textit{ oppure } t_i^{-1} \in X\}$$

L'insieme che contiene i prodotti finiti di elementi di X oppure i cui inversi sono in X.

Dimostrazione:

1. $\langle X \rangle$ contiene X, $r = 1, t_i \in X$
2. $\langle X \rangle \leq G$
   - contiene 1_G: sia $\overline{x} \in X$ qualunque $\Rightarrow \overline{x} \in \langle X \rangle, \overline{x}^{-1} \in \langle X \rangle$ e $\overline{x} \cdot \overline{x}^{-1} = 1_G \in \langle X \rangle$
   - $\langle X \rangle$ è chiuso rispetto al prodotto di G
   - Se $t_1, t_2, ..., t_r \in \langle X \rangle$, e t_1

TODO:CONTROLLARE APPUNTI

7.4 $\langle X \rangle$ è il più piccolo sottogruppo che contiene X

Da dimostrare in proprio, lo ha dato come esercizio

7.5 Defizione: ordine (periodo)

Se un elemento di G ha periodo finito, allora si chiama *ordine* (o periodo) di g il più piuccolo positivo tale che $g^m = 1_G$

7.6 Definizione: gruppo ciclico

Un gruppo G si dice ciclico se esiste $g_0 \in G$ tale che $G = \langle g_0 \rangle$ *(gruppo che viene generato da un solo elemento).*

7.7 Proposizione

Il sottogruppo generato da un elemento (in un gruppo ciclico) è commutativo.
Dimostrazione:

$$\langle g \rangle = \{g^h : h \in \mathbb{Z}\}$$

$$x = g^h,\ y = g^k \quad h, k \in \mathbb{Z}$$

$$x \cdot y = g^h g^k = g^{h+k} = g^k g^h = y \cdot x$$

7.8 Proposizione

Sia G gruppo:

1. Se $g \in G$ ha periodo infinito ($\nexists\ h > 0 : g^h = e$) allora $\exists\ h, k \in \mathbb{Z}, h \neq k,\ g^h \neq g^k$: il gruppo ciclico generato da G, $\langle g \rangle \cong \mathbb{Z}$.

2. g ha periodo finito.
   Se n=periodo di $g = o(g) = ord_G(g)$ ovvero $n = min\{k > 0 : g^k = e\}$ allora $\langle g \rangle = \{e, g, g^2, ..., g^{n-1}\}$ dove queste potenze sono tutte distinte.

Dimostrazione pt.1: Dimostro che se:

$$g^h = g^k \Rightarrow h = k$$

infatti moltiplico per g^{-k} ed ho:

$$g^{h-k} = g^{k-k} \Rightarrow g^{h-k} = g^0 = e$$

ma g è aperiodico

$$\Rightarrow h - k = 0 \Rightarrow h = k$$

Dimostrazione pt.2: so che $\langle g \rangle = \{g^h : h \in \mathbb{Z}\}$ devo dimostrare che ogni elemento g^h sta già in $\{e, g, g^2, ...g^{n-1}\}$.

Divido h per n:

$$h = nq + r,\ \ 0 \leq r < n$$

$$\Rightarrow g^h = g^{nq+r} = g^{nq} g^r = (g^n)^q g^r = e^q g^r = e g^r = g^r$$

ed r è un numero $0 \leq r < n$ e quindi è una potenza dell'insieme.

7.9 Proposizione: sottogruppi di un gruppo ciclico

0. Sottogruppi di $(\mathbb{Z}, +)$: sono tutti e soli della forma

$$H = m\mathbb{Z} = \{mh : h \in \mathbb{Z} = \langle m \rangle\}, \quad m \in \mathbb{N}$$

.
Non dimostrato.

1. I sottogruppi di $\langle g \rangle$ con $g \in (G, \cdot)$, g aperiodico, sono tutti e soli della forma:

$$H = \langle g^m \rangle$$

per qualche $m \in \mathbb{Z}$.
Non dimostrato.

2. I sottogruppi di un gruppo ciclico generato da un elemento di ordine n ($g^n = e$, n più piccolo positivo con $g^n = e$) sono anch'essi ciclici e generati da $\langle g^h \rangle,\ h|n$.

7.10 Osservazione

I sottogruppi di un gruppo ciclico finito verificano la seguente condizione:

$$H \leq \langle g \rangle \Rightarrow |H|\,|o(g) = |\langle g \rangle|$$

L'ordine di un sottogruppo $H \leq \langle g \rangle$ divide l'ordine dell'elemento g, che è anche l'ordine del gruppo.

7.11 Proposizione

In S_n, sia $\sigma(C_1)(C_2)...(C_k)$ la fattorizzazione di σ come prodotto dei suoi cicli disgiunti. Allora se m_i =lunghezza di C_i

$$ordine(\sigma) = mcm(m_1, m_2, ..., m_k)$$

7.12 Proposizione

$G = C_n = \langle g \rangle$ gruppo ciclico generato da un elemento di ordine $n = \{id, g, g^2, ..., g^n\}$.
Tutti e soli i generatori di C_n sono le potenze di g con esponente coprimo con n.
Generatori: $g^t,\ (t, n) = 1$

7.13 Teorema di Lagrange

Se G è un gruppo finito, allora l'ordine di un sottogruppo divide l'ordine del gruppo:

$$H \leq G \Rightarrow |H|\,|\,|G| = o(H)|o(G)$$

Oss: non vale sempre il viceversa.

Se $d|o(G) \Rightarrow \exists H \leq G,\ o(H) = d$

Dimostrazione: Siano $n = o(G)$ e $m = o(H)$, i il numero di calssi laterali destre modulo H.
$Ci_d =$ indice del sottogruppo H nel gruppo G.
$i = |G_{/\sim d}| =$ numero di classi laterali. Esistono $a_1, a_2, ..., a_i$ rappresentanti distinti delle classi laterali.

$$G = Ha_1 \dot{\cup} Ha_2 \dot{\cup} ... \dot{\cup} Ha_i \Rightarrow |G| = o(G) =$$

$$= \sum_{j=1}^{i} |Ha_j| = \sum_{j=1}^{i} |H| = i \cdot |H| = i \cdot m$$

cioè ho $n = i \cdot m$. $ord(G)$ =numero classi laterali destre$\cdot ord(H)$.
Da questa relazione deduco che:

1. $ord(H)|ord(G)$
2. $i|o(G)$

Oss: ripeto tutto per le classi laterali sinistre $i_s \cdot m = n$.

7.13.1 Corollario 1

Se $|G| = p$ primo, allora gli unici sottogruppi di G sono $H = \{e\}$ oppure $H = G$ (non ci sono sottogruppi intermedi).

7.13.2 Corollario 2

Se $|G| = primo$, allora G è ciclico (in particolare è abeliano).
Dimostrazione: Se $|G| = p$ primo> 1.
Sia $x_0 \in G, x_0 \neq e$. Sia $H = \langle x_0 \rangle \neq \{e\}$ $(H = \{e, x_0, x_0^2 ...\})$, per il *corollario 1*:

$$H = G \Rightarrow G = \langle x_0 \rangle$$

7.14 Definizione: indice di un sottogruppo

L'indice di un sottogruppo H in un gruppo G è:

$$i = i_s = i_d$$

e si denota:

$$i = [G : H]$$

8 Classi laterali di un sottogruppo

8.1 Definizione: congruenza destra modulo

Sia $(G, \cdot)$ un gruppo, sia $H \leq G$ sottogruppo.

Definiamo congruenza destra modulo H la relazione così definita:

$$\forall\, a, b \in G : a \sim_d b \Leftrightarrow a \cdot b^{-1} \in H$$

8.2 Proposizione

$\sim_d$ $(mod\ H)$ è una relazione di equivalenza.

Dimostrazione:

- (R) $a \sim_d a$?
$$a \cdot a^{-1} = e\ \in H$$
- (S) $a \sim_d b \Rightarrow b \sim_d a$?
$$ab^{-1} \in H$$
H sottogruppo:
$$(ab^{-1})^{-1}\ \in H$$
$$\Rightarrow (b^{-1})^{-1} \cdot a^{-1} = b^{-1} \cdot a \Rightarrow b \sim_d a$$
- (T) $a \sim_d b$ e $b \sim_d c \Rightarrow a \sim_d c$?
$$ab^{-1} \in H\ e\ bc^{-1} \in H$$
$$(ab^{-1})(bc^{-1}) \in H$$
H è chiuso rispetto al prodotto
$$(ab^{-1})(bc^{-1}) = ac^{-1} \Rightarrow a \sim_d c$$

8.3 Insieme quoziente

Dato $a \in G$: $[a]_{\sim_d} = H \cdot a$ dove $Ha = \{ha : h \in H\}$, $H = \{e, h_1, h_2 ...\}$, $Ha = \{e \cdot a, h_1 \cdot a, ...\}$.

Dimostrazione: devo provare $1.Ha \subseteq [a]_{\sim_d}$ e $2.[a]_{\sim_d} \subseteq Ha$.

1.
$$b \in Ha$$
$$\Leftrightarrow \exists h : b = ha$$
$$\text{moltiplicando per } a^{-1}$$
$$\Leftrightarrow h = ba^{-1}$$
$$\Leftrightarrow ba^{-1} \in G$$
$$\Leftrightarrow b \sim_d a \Leftrightarrow b \in [a]_{\sim_d}$$

è la stessa di sopra ma partendo dalla fine verso l'inizio.

8.4 Proposizione

Tutte le classi laterali destre hanno la stessa cardinalità.

Dimostrazione: dimostro che $|Ha| = |H|$ $\forall a \in A$ ($|Ha| = [a]_{\sim_d}$, per transitività $|Ha| = |Hb|$.
Sia

$$\varphi : H \to Ha$$
$$h \to ha$$

- Suriettiva: ogni elemento di Ha è del tipo ha per qualche $h \in H$.
- Iniettiva: $\varphi(a) = \varphi(h') \Rightarrow ha = h'a \Rightarrow$ per la cancellatività nel gruppo $\Rightarrow h = h'$

8.5 Definizione: congruenza sinistra modulo

$$\forall\ a, b \in G,\ \ a \sim_s b \Leftrightarrow b^{-1}a \in H$$

La classe laterale sinistra : $[a]_{\sim_s} = aH = \{ah : h \in H\}$

9 Omomorfismi

9.1 Isomorfismo

Dati $(G, *)$ e $(H, \cdot)$ due gruppi, un isomorfismo di G in H è

- $\varphi : G \to H$ una biiezione.
- φ rispetta le operazioni di gruppo, cioè:

$$\forall\, a, b \in G : \varphi(a * b) = \varphi(a) \cdot \varphi(b), \;\; \varphi(a) \; e \; \varphi(b) \in H$$

Si dice che G è isomorfo ad H e si scrive $G \cong H$.

9.2 Omomorfismo

Se $\varphi : G \to H$ conserva le operazioni di G e H, φ si chiama omomorfismo, ovvero un omomorfismo è un'applicazione tale che:

$$\forall\, a, b \in G : \varphi(a * b) = \varphi(a) \cdot \varphi(b)$$

9.3 Epimorfismo

Se φ è suriettiva, φ si chiama epimorfismo.

9.4 Monomorfismo

Se φ è iniettiva, si chiama monomorfismo.

9.5 Isomorfismo 2

Se φ è biunivoca, allora φ si chiama isomorfismo.

9.6 Proposizione

L'isomorfismo tra gruppi è una relazione di equivalenza.

9.7 Kernel/Nucleo

Se l'applicazione φ è un omomorfismo, allora viene definito *nucleo* di $\varphi \subseteq G$

$$Ker(\varphi) : \{x \in G : \varphi(x) = e'\}$$

dove:
$e =$ l'elemento neutro di G
$e' =$ l'elemento neutro di G'

9.8 Proposizione

Dato $\varphi : G \to G'$ omomorfismo, allora:

1. $\varphi(e) = e'$
2. $\varphi(g^{-1}) = (y(g))^{-1}$
3. $Ker(\varphi) \leq G$
4. $Im\varphi \leq G'$

Dimostrazione 1: Per dimostrare che $\varphi(e)$ è l'elemento neutro di e' devo mostrare che $\forall y \in G'$: $\varphi(e) \cdot y = y$; moltiplicando per y^{-1} (la cancellazione in G') di ottiene:

$$\varphi(e)\varphi\varphi^{-1} = \varphi\varphi^{-1}$$
$$\Rightarrow \varphi(e) = e'$$

Dimostrazione 2: lasciata per esercizio

Dimostrazione 3: $Ker\varphi \leq G$?

- contiene e: è il punto 1: infatti $\varphi(e) = e'$
- è chiuso rispetto al prodotto: siano $a, b \in Ker\varphi$ e verifichiamo che $a * b \in Ker\varphi$:

$$a \in Ker\varphi \Rightarrow \varphi(a) = e'$$
$$b \in Ker\varphi \Rightarrow \varphi(b) = e'$$
$$a * b : \ \varphi(a * b) = \varphi(a)\varphi(b) = e' \cdot e' = e'$$
$$\Rightarrow a * b \in Ker\varphi$$

- è chiuso rispetto agli inversi: sia $a \in Ker\varphi$ (cioè $\varphi(a) = e'$) devo provare che $a^{-1} \in Ker\varphi$:

$$\varphi(a^{-1}) = (\varphi(a))^{-1} = (e')^{-1} = e'$$

  quindi $a^{-1} \in Ker\varphi$

Dimostrazione 4 TODO: Ricontrollare appunti

9.9 Omomorfismo di anelli

Se $(A, +, \cdot)$ è $(A', +, \cdot)$ sono anelli $0_A, 0_{A'}$ i corrispettivi elementi neutri, un omomorfismo di anelli è un'applicazione:

$$\varphi : A \to A'$$

tale che:

- $\varphi(x_1 + x_2) = \varphi(x_1) + \varphi(x_2) \quad \forall x_1, x_2 \in A$
- $\varphi(x_1 \cdot x_2) = \varphi(x_1) \cdot \varphi(x_2)$

$$Ker\varphi = \{x \in A : \varphi(x) = 0'_A\} \subseteq A \; sottoanello$$

TODO: *qui c'è un insieme che non ho capito

9.10 Proposizione

$\varphi : (G, *) \to (G', \cdot)$ omomorfismo di gruppi, allora:

$$\varphi \; iniettiva \Leftrightarrow Ker\varphi = \{e\}$$

$$\varphi \; iniettiva \leftrightarrow |\varphi^{-1}(y)| \leq 1 \; \forall \; y$$

$$\varphi \; iniettiva + omomorfismo \Leftrightarrow \varphi^{-1}(e^{-1}) = e$$

Dimostrazione: $Ker = Ker\varphi \leq G'$
Consideriamo la congruenza modulo il segno (?) k

$$a \sim_d b \Leftrightarrow ab^{-1} \in K (= Ker\varphi) \Leftrightarrow \varphi(a * b^{-1}) = e'$$

φ è un morfismo:

$$\Leftrightarrow \varphi(a)\varphi(b^{-1}) = e$$

$$\Leftrightarrow \varphi(a)(\varphi(b))^{-1} = e'$$

moltiplicando per $\varphi(b)$

$$\Leftrightarrow \varphi(a) = \varphi(b)$$

$$\Leftrightarrow \varphi \; iniettiva$$

9.11 Proposizione

$G, G' \quad \varphi : G \to G'$ omomorfismo, allora:

1. Se G finito, allora l'ordine $Im\varphi$ divide l'ordine di G (ed anhe di G', se G' è finito).
2. Se G è ciclico, allora $Im\varphi$ è un sottogruppo ciclico di G'
3. Se $g \in G$ ha periodo finito, allora il perodo di $\varphi(g)$ divide l'ordine di g

10 Spazi Vettoriali

10.1 Definizione spazio vettoriale

Uno spazio vettoriale V su un campo K è

- Un insieme nn vuoto V, in cui sono definite due operazioni, di cui una interna ed una esterna.
  Interna: somma $+$:
  $$V \times V \to V$$
  $$(v, w) \mapsto v + w$$
  Esterna: prodotto $\cdot$ per uno scalare:
  $$K \times V \to V$$
  $$(c, v) \mapsto c \cdot v$$
- $(V, +)$ è un gruppo commutativo
- $K \times V \to V$ e $(c, v) \mapsto c \cdot v$ tale che:
  - distributività per vettori:
    $$\forall c \in K, \forall v, w \in V$$
    $$c(v + w) = cv + vw$$
    $$(v + w)c = vc + wc$$
  - associatività per gli scalari:
    $$\forall c, d \in K, \forall v \in V$$
    $$c(dv) = (cd)v$$
- distributività per gli scalari:
  $$\forall c, d \in K, v \in V$$
  $$(c + d)v = cv + dv$$
- $1 \cdot v = v$

10.2 Scalare

E' un elemento del campo.

10.3 Sottospazio vettoriale

Un sottospazio vettoriale di uno spazio vettorialo V su R è un sottoinsieme $W \subseteq V$ non vuoto tale che: W rispetto le stesse operazioni di V sia esso stesso uno spazio vettoriale.

- Equivalentemente si deve avere:
  1. $(W, +)$ è un sotto gruppo di $(V, +)$
  2. chiuso rispetto alla moltiplicazione per uno scalare
- Equivalentemente:
  1. $\forall\, u, v \in W$: $u - v \in W$ $[a \cdot b^{-1} \in G]$
  2. $\forall\, \alpha \in \mathbb{R}, v \in W$: $\alpha \cdot v \in W$
- Equivalentemente:
  1. $\forall\, u, v \in W : u - v \in W$
  2. $\forall \alpha \in \mathbb{R}, \forall v \in W : \alpha v \in W$
     (Se $\alpha = -1, v \in W$ allora $-v \in W$
     $u \in W$ allora $u - (-v) = u + v$)
- Equivalentemente $W \subseteq V$ è un sottospazio vettoriale $\Leftrightarrow$

  1* $\forall\, u, v \in W : u + v \in W$

  2* $\forall\, \alpha \in \mathbb{R}, \forall v \in W : \alpha v \in W$

10.4 Proposizione

$W \subseteq V, W \neq \emptyset$ è un sottospazio vettoriale $\Leftrightarrow$:

$$\forall\, \alpha\beta \in \mathbb{R}, \forall\, u, v \in W :\ \alpha u + \beta v \in W$$

$\alpha u + \beta v$ si chiama **combinazione lineare** di u e v.

Dimostrazione: la combinazione lineare è equivalente a $1*$ e $2*$. Supponiamo che $\alpha u + \beta v \in W$ $\forall\, \alpha\beta \in \mathbb{R}, \forall\, u, v \in W$
$2* \rightarrow$ in particolare è vero se prendo $\alpha = \alpha, \beta = 0$: $\alpha u + \beta v = \alpha u \in W$.
$1* \rightarrow$ in particolare, se prendo $\alpha = 1, \beta = -1$: so che $1 \cdot u + (-1) \cdot v = u - v \in W$.

10.5 Definizione: traccia

Data una matrice quadrata $A = [a_{i,j}]$ si chiama traccia della matrice il valore (scalare in $\mathbb{R}$) definito da:

$$tr(A) = a_{11}, a_{22}, a_{33} + ... + a_{nn}$$

(è la somma degli elementi della diagonale).

10.6 Definizione: combinazione lineare

Dati $v_1, ...v_t \in V$ vettori di uno spazio vettoriale V su $\mathbb{R}$ dati t scalari $c_1, c_2, ..., c_t \in \mathbb{R}$, il vettore $v = c_1v_1 + c_2v_2 + ... + c_tv_t$ si chiama combinazione lineare di vettori $v_1, ..., v_t$ tramite gli scalari $c_1, ..., c_t$.

10.7 Proprietà di calcolo negli spazi vettoriali

V spazio vettoriale su K, 0 è lo zero del campo, $0_V = \underline{0}$ è l'elemento neutro del gruppo (V, t)

- $0v = \underline{0}$ vettore nullo $\forall v \in V$
- $(-c)v = -(cv)\ \forall\ v \in V, \forall c \in \mathbb{R}$
- $c\underline{0} = \underline{0}$
- Se $cv = \underline{0}$ allora $c = 0$ oppure $v = \underline{0}$

10.8 Definizione

w è combinazione lineare di $v_1, v_2, ..., v_t$ se esistono degli scalari $c_1, c_2, ..., c_t \in \mathbb{R}$ tali che:

$$w = c_1v_1 + ... + c_tv_t$$

10.9 Osservazione: combinazione lineare banale

Lo "zero" vettoriale è sempre combinazione lineare di un insieme $\{v_1, ..., v_t\}$ di vettori qualunque:

$$\underline{0} = 0v_1 + 0v_2 + ... + 0v_t$$

10.10 Definzione: linearmente dipendente

Un insieme di vettori $\{v_1, ..., v_n\}$ è linearmente dipendente (sul campo di V) $\Leftrightarrow$ esistono coefficienti $c_1, ..., c_n \in K$ non tutti nulli, tali che:

$$c_1v_1 + c_2v_2 + ... + c_nv_n = \underline{0}$$

10.11 Osservazione

Se almeno uno dei coefficienti $\{c_1, ..., c_n\}$ è non nullo (sia $C_j \neq 0$), allora si può scrivere (partendo dalla precedente *linearmente dipendente*):

$$c_jv_j = -c_1v_1 - c_2v_2 - ... - c_{j-1}v_{j-1} - c_{j+1}v_{j+1} - .... - c_nv_n$$

e $C_j \neq 0 \Rightarrow \exists c_j^{-1}$ allora:

$$v_j = -\frac{c_1v_1}{c_j} - \frac{c_2v_2}{c_j} - ... - \frac{c_nv_n}{c_j}$$

10.12 Osservazione

$\{v_1, ...v_n\}$ è un insieme linearmente **indipendente** $\Leftrightarrow \underline{0} = c_1v_1 + ... + c_nv_n \Leftrightarrow c_1 = c_2 = ... = c_n = 0$.

Ovvero: $\{v_1, ..., v_n\}$ sono vettori linearmente indipendenti $\Leftrightarrow$ l'unica combinazione lineare di $v_1, ..., v_n$ è la combinazione lineare banale.

10.13 Osservazione

Il vettore nullo $\underline{0}$ di V è sempre linearmente dipendente da qualunque insieme finito di vettori.

Infatti sia $\{u_1, ...u_z\} \subseteq V$ allora:

$$\underline{0} = 1 \cdot \underline{0} = 0u_1 + 0u_2 + ... + 0u_t$$

(un modo equivalente: $0u_1 + 0u_2 + ... + 0u_t - 1 \cdot \underline{0} = \underline{0}$)

10.14 Osservazione

Se $S \subseteq V$ con $\underline{0} \in S$, $S = \{\underline{0}, v_1, ..., v_k\}$ allora S è un insieme di vettori dipendenti: infatti c'è la dipendenza

$$1 \cdot \underline{0} = 0v_1 + 0v_2 + ... + 0v_k$$

10.15 Osservazione

La proprietà di essere indipendente di $S \subseteq V$, $S = \{v_1, ..., v_t\}$ si eredita ai sottoinsiemi, cioè:

$$\forall\, T \subseteq S,\ S \textit{ indipendente} \Rightarrow T \textit{ indipendente}$$

$\{v_1\}$ è un insieme indipendente $\Leftrightarrow v_1 \neq 0$; $\{\underline{0}\}$ è indipendente.

10.16 Sottospazio generato da: span

Dati $v_1, v_2, ..., v_t$ vettore di V (spazio vettoriale su un campo) lo *span* dei vettori $v_1, ..., v_t$ è il più piccolo sottospazio vettoriale di V che contiene $v_1, ...v_t$

$$Span(v_1, ..., v_t) = \bigcap_{W \leq V\ \{v_1 ... v_t\} \in W} W$$

Altra notazione Span: $< v_1, ...v_t >$

10.17 Proposizione

$$Span(v_1, ...v_t) = \{\sum_{i=1}^{t} \alpha_i v_i : \alpha_i, ..., \alpha_t \in K\}$$

Dimostrazione data per esercizio

10.18 Sistema di generatori

Dato V su K (es. $K = \mathbb{R}$), i vettori $\{v_1, ...v_t\}$ sono un sistema di generatori (o insieme di generatori) per V se

$$V = Span(v_1, ..., v_t)$$

Se $W \subseteq V$ è un sottospazio, allora $\{u_1, ..., u_k\}$ sono generatori (sistema di generatori) per W se

$$W = Span(u_1, ..., u_k)$$

10.19 Basi di spazi vettoriali

Dato V su K, un insieme $B = \{v_1, ..., v_n\} \subseteq V$ si chiama base di V se:

- $V = Span(v_1, ..., v_n)$ cioè B sono generatori per V.
- $\{v_1, ..., v_n\}$ sono indipendenti.

10.20 Spazio finitamente generato

Uno spazio vettoriale V(su K), si dice finitamente generato se ammette un insieme finito di generatori.

10.21 Proposizione

$B = \{v_1, ..., v_n\}$ é una base di $V \Leftrightarrow \forall v \in V \exists! \ (c_1, ..., c_n), c_i \in \mathbb{R}$ con
$v = c_1v_1 + c_2v_2 + ... + c_nv_n$

Dimostrazione$\Rightarrow$

1. Ipotesi: $B = \{v_1, ..., v_n\}$ é una base di V
2. Tesi: $v = c_1v_1 + c_2v_2 + ... + c_nv_n$

Sia $v \in V$. Siccome B è una base, allora è un insieme di generatori di $V \Rightarrow v \in Span(v_1, ..., v_n) \Rightarrow \exists c_1, ..., c_n$ con $v = c_1v_1 + ... + c_nv_n$
Perchè sono unici? Siano $(d_1, ..., d_n)$ con

$$v = d_1v_1 + ... + d_nv_n$$

$$v = c_1v_1 + ... + c_nv_n$$

$$\Rightarrow v - v = 0 = d_1v_1 + ... + d_nv_n - (c_1v_1 + ... + c_nv_n) =$$

$$= (d_1 - c_1)v_1 + ... + (d_n - c_n)v_n$$

ma $v_1, ..., v_n$ sono indipendenti $\Rightarrow$ i coefficienti (d_kv_k) sono tutti nulli.

Dimostrazione $\Leftarrow$ *fare per esercizio*

10.22 N-upla delle coordinate di v in base B

Data $B = \{v_1, ..., v_n\}$ una base ordinata di V, se $v = c_1v_1 + ... + c_nv_n$ allora il vettore colonna $[c_1 \ ... \ c_n] \in \mathbb{R}^n$ si chiama vettore delle coordinate di v in base B.

10.23 Corollario

Fissata una base $B = \{v_1, ..., v_n\}$ di V l'applicazione $\varphi : V \to K^n$ (K è il campo di V) che manda v in $\varphi(v) = [c_1 \ ... \ c_n]$ (cioè il vettore nelle sue coordinate in base B) è una biiezione.

10.24 Teorema: esistenza di una base

Se V è uno spazio vettoriale finitamente generato (cioè se $V = Span(v_1, ..., v_h)$) allora esiste una base $\{w_1, ..., w_n\}$ di V.
Non dimostrato.

10.25 Proposizione

Date due basi $B = \{v_1, ..., v_n\}$ e $B = \{w_1, ..., w_m\}$ di V allora $n = m$.

10.26 Dimensione di V

Se V è finitamente generato, allora si chiama dimensione di V la cardinalità di una qualunque base di V.

10.27 Osservazione (notazione)

Se la dimensione di V è n, allora $\varphi : V \to K^n$ si scrive $dim_k V = n$ se $|B| = n$.

10.28 Teorema del completamento di una base

Sia $B = \{v_1, ..., v_n\}$ una base di V, e sia $\{w_1, ..., w_p\}$ con $\{p \leq n\}$ un insieme di vettori indipendenti. Allora posso completare $\{w_1, ..., w_p\}$ con $(n-p)$ vettori di B a formare una base (ovvero posso sostituire p vettori di B un altro insieme di p vettori indipendenti).
Dimostrazione fatta parzialmente da vedere per lode.

10.29 Teorema

Le seguenti condizioni sono equivalenti tra loro per un insieme $B = \{v_1, ..., v_n\} \subseteq V$ di n vettori:

1. B è una base.
2. B è un insieme di generatori minimale (cioè ogni sottoinsieme S proprio di V genera un sottospazio $Span(S) \not\leq V$)

3. B è un insieme di vettori linearmente indipendenti massimale (cioè ogni $T \supsetneq B$ insieme di vettori che contiene B non è più indipendente).

10.30 Corollario

Se V è finitamente generato e $B = \{v_1, ..., v_n\}$ $B' = \{v'_1, ..., v_m\}$ sono basi di V allora $|B| = |B'|$ $(n = m)$.

Dimostrazione: per assurdo $m < n$, allora con il teorema del completamento costruisco $B'' = B' \cup \{n - m \text{ } vettori\}$. B' è una base ma per il pt.3 (teorema precedente) B' è un insieme massimale $\Rightarrow$ contraddizione.

10.31 Osservazioni

- Se $dim_K V = n$ allora ogni sottoinsieme di n vettori indipendenti è anche un insieme di generatori.
- Se $dim_K V = n$ allora ogni insieme di n che generano V è anche un insieme indipendente (cioè una base).
- Se $W \leq V$, sottospazio di V con $dim_K V = n$ allora:
  - $dim_K W \leq dim_K V$
  - $dim_K W = dim_R V \Leftrightarrow W = V$
  - $W \neq \{0_V\} \Leftrightarrow dim_K W > 0$

10.32 Somma di sottospazi

Dati $U, W \leq V$ (V spazio vettoriale su R):

1. L'intersezione $U \cap W$ è anche un sottospazio di V

$$U \cap W \{v \in V : v \in U \wedge v \in W\}$$

   Dimostrazione per esercizio

2. (L'unione di due sottospazi non è, in generale, un sottospazio (a meno che non siano uno contenuto nell'altro)). Il più piccolo sottospazio di V che contiene sia V che W si chiama la **somma** di U e W e si denota:

$$U + W = Span(U \cup W)$$

10.33 Proposizione

$$U + W = \{u + w : u \in U, w \in W\}$$

Per esercizio verificare che u+w è un sottospazio che contiene $U \cup W$ *e* $Span(U + W)$

10.34 Teorema di Grossman

$dim_K(U+V) = dim_K U + dim_K W - dim_K(U \cap W)$

10.35 Somma diretta di sottospazi

Quando $U \cap V = \{0_V\}$, cioè ha dimensione 0, allora si parla di somma diretta di sottospazi e si scrive:

$$U \oplus W$$

10.36 Proposizione

Se $U \cap V = \{0_V\}$ allora ogni vettore di $U \oplus W$ si scrive come somma di un elemento di U più un elemento di W in modo unico.

Dimostrazione: supponiamo che $v_0 \in U + W$ si scriva in due modi diversi:

$$v_0 = u + w = u' + w' \ \ (con\ u, u' \in U;\ w, w' \in W)$$

$$\Rightarrow v_0 - v_0 = 0 = u + w - (u' - w') =$$

$$(u + u') + (w - w') = 0$$

$$\Rightarrow \in U \cap W = \{0_V\}$$

$$\Rightarrow u - u' = 0 \Rightarrow u = u'$$

$$\Rightarrow w - w' = 0 \Rightarrow w = w'$$

11 Sistemi di equazioni lineari

11.1 Scrittura

Ogni sistema di equazioni lineari si può scrivere nella forma:

$$AX = K$$

X è la colonna delle incognite, K la colonna dei termini noti del sistema

11.2 Risolvere sistema di equazioni

Una soluzione del sistema è una n-upla di reali i cui valori $s_1, ..., s_n$ sostituiti alle incognite le rendano tutte vere. cioè:

$$S = \begin{bmatrix} s_1 \\ ... \\ s_n \end{bmatrix}$$

con

$$A \cdot S = K$$

11.3 Sistemi equivalenti

Due sistemi $AX = K$ e $BX = K$ sono equivalentei se hanno esattamente le stesse soluzioni.

11.3.1 Operazioni elementari di riga

- $L = L_{ij}$ scambio riga i e riga j
- $L = L_i(c)$ moltiplico la riga i per la costante c
- $L = L_{ij}(c)$ sostituisco alla riga i la riga ottenuta sommando ad i c volte la riga j, $c \neq 0$

11.4 Equivalenza per riga

Due matrici A e B dello stesso ordine $n \times m$ sono equivalenti per riga se B si ottiene da A per applicazione successiva di un numero finito di *operazioni elementari* di riga, cioè se:

$$B = L_k ... L_2 L_1(A)$$

e si scrive:

$$A \sim B$$

11.5 Proposizione

L'equivalenza per riga è una relazione di equivalenza. *Dimostrazione sulle note della prof.*

11.6 Proposizione

Siano A, B matrici $m \times n$, se una successione di operazioni elementari di riga trasforma A in B, allora le stesse operazioni trasformano la matrice identica in una matrice P tale che $B = P \cdot A$.
In altre parole

$$[A|I] \sim [B|P]$$

11.7 Matrice identica

$$I = \begin{bmatrix} 1 & 0 & 0 & ... & 0 & 0 \\ 0 & 1 & 0 & ... & 0 & 0 \\ 0 & 0 & 1 & ... & 0 & 0 \\ & & & ... & & \\ & & & ... & & \\ 0 & 0 & 0 & ... & 0 & 1 \end{bmatrix}$$

11.8 Corollario

Se $A \in M_n(\mathbb{R})$ ed è invertibile, allora l'inversa si trova applicando la riduzione per righe alla matrice A aumentata della matrice I, cioè:

$$[A|I] \sim [I|A^{-1}]$$

11.9 Teorema

Per ogni matrice A $m \times n$ esiste una matrice R $m \times n$:

- ridotta a scala
- $A \sim R$ (riga equivalente ad A)

11.10 Rango

Si chiama rango di una matrice A il numero di pivot di una ridotta scala R riga-equivalente ad A

11.11 Pivot

Primo elemento non nullo in una riga della matrice.

11.12 Rango pieno

Una matrice A è di rango pieno se $rg(A) = m$ (m=massimo possibile cioè il numero di righe).

11.13 Proposizione: proprietà del rango

Il rango di A ha le seguenti proprietà:

1. Se $A \sim B$ allora $rg(A) = rg(B)$ $(A \sim R \Rightarrow B \sim R)$
2. Se A è di ordine $m \times n$, allora $rg(A) \leq min\{m, n\}$
3. $rg(A \cdot B) \leq min\{rg(A), rg(B)\}$
4. $rg(A^t) = rg(A)$, dove A^t è la matrice trasoposta di A definita: $(A^t)_{ij} = a_{ij}$ *(scambia le righe con le colonne)*.

11.14 Teorema: Rouchè-Capelli

Dato un sistema $AX = K$, allora:

1. Se $rg([A|K]) > rg(A)$, allora il sistema è incompatibile: non ci sono soluzioni.
2. Se $rg([A|K]) = rg(A)$, allora ho due casi:
   (a) Se $n = r = rg(A)$: rango massimo, c'è una sola soluzione.
   (b) Se $r = rg(A) < n$: ho infinite soluzioni che saranno paramentriche, con tanti parametri quante le colonne non pivot (tanti parametri quanto $n - rg(A)$).

12 Studio dei sistemi omogenei

Le matrici con una sola colonna sono scritte come righe con un pedice: $[valori]_{colonna}$.

12.1 Proposizione

Sia $AX = 0$ un sistema lineare omogeneo (con $A \in M_{m\times n}(\mathbb{R})$. Allora

$$W = \{X = [x_1...x_n]_{colonna} \in \mathbb{R} : AX = 0\}$$

L'insieme delle soluzioni del S.L.O. è un sottospazio di R^n

Dimostrazione Se X, X' sono in W allora $\alpha X + \beta X' \in W$? $A(\alpha X + \beta X') = \alpha AX + \beta AX' = \alpha\underline{0} + \beta\underline{0} = \underline{0}$

12.2 Teorema: Struttura sulle soluzioni di un sistema

Sia $AX = b$ un sistema lineare (b colonna dei termini noti). Sia $v_0 \in \mathbb{R}^n$ una soluzione del sistema $AX = b$. $v = \begin{pmatrix} v_1 \\ ... \\ v_n \end{pmatrix}$ (una soluzione "particolare") Allora ogni altra soluzione di $AX = b$ si scrive nella forma

$$v = v_0 + w \;\; (\textit{soluzione generale})$$

al variare di $w \in W = \{X : AX = \underline{0}\}$ cioè al variare di w nelle soluzioni del sistema lineare omogeneo associato $AX = \underline{0}$.

$$(Av_0 = b,\; Aw = \underline{0}$$
$$\Leftrightarrow A(v_0 + w) = b \Rightarrow Av_0 + Aw = b + \underline{0} = b)$$

12.3 Nota importante

$A(X + Y) = AX + AY$: la moltiplicazione per una matrice è quindi lineare.

13 Applicazioni lineari

13.1 Definizione: applicazione lineare (trasformazione lineare o homomorfism of vector space)

Un'applicazione lineare è un'applicazione $T : V \to W$ di spazi vettoriali su K tale che $\forall v, v_1, v_2 \in V$, $\forall \lambda \in K$ si ha:

1. $T(v_1 + v_2) = T(v_1) + T(v_2)$ (T è additiva)
2. $T(\lambda \cdot v) = \lambda \cdot T(v)$ (T è omogenea)

(additiva+omogenea = è lineare).
In altre parole T conserva le operazioni di spazio vettoriale.

13.2 Proposizione

Punti $1 + 2 \Leftrightarrow 3 :\ \forall \lambda\mu \in K, \forall v_1, v_2 \in V$

$$T(\lambda v_1 + \mu v_2) = \lambda T(v_1) + \mu T(v_2)$$

T manda combinazioni lineari in combinazioni lineari (con gli stessi scalari) dei trasformati.

13.3 Definizione

Fissata $A \in \mathcal{M}_{mn}(\mathbb{R}) : A = \begin{bmatrix} a_{11} & ... & a_{1_n} \\ & ... & \\ a_{m1} & ... & a_{mn} \end{bmatrix}$, sia $L_A : \mathbb{R}^n \to \mathbb{R}^m$ definita da:

$$X \begin{bmatrix} x_1 \\ ... \\ x_n \end{bmatrix} \mapsto L_A(x) := AX = \begin{bmatrix} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n \\ ... \\ a_{m_1}x_1 + a_{m_2}x_2 + ... + a_{mn}x_n \end{bmatrix} \in \mathbb{R}^n$$

La trasformazione L_A è la moltiplicazione (a destra) per A:

$$L_A : X \mapsto AX$$

ad ogni matrice A corrisponde una trasformazione lineare L_A.

Per esercizio: dimostrare che $L_A : \mathbb{R}^n \to \mathbb{R}^m$ è lineare.

- $L_A(X + Y) = L_A(X) + L_A(Y)$*? (dimostrazione su appunti)*
- $L_A(\lambda X) = \lambda L_A(X)$?

13.4 Definizione

Data una trasformazione lineare $T : V \to W$, restano determinati due sottoinsiemi:

- Il nucleo di T: $KerT$

$$KerT = \{v \in V : T(v) = 0_W\} \subseteq V$$

- L'immagine di T: ImT

$$ImT = \{T(v) : v \in V\} \subseteq W$$

13.5 Proposizione (risolvere per esercizio)

1. $KerT \leq V$
2. $ImT \leq W$
3. T suriettiva $\Leftrightarrow ImT = W$
4. T iniettiva $\Leftrightarrow KerT = \{0\}$

13.6 Osservazione (!)

Calcolare il nucleo di un'applicazione lineare corrisponde a risolvere un sistema omogeneo.

13.7 Proposizione

Un'applicazione lineare $T : V \to W$ è definita univocamente (ovvero è determinata) quando si conoscono le immagini di T sui vettori $\{v_1, ..., v_n\}$ di una base di V, se $dimV = n$: ovvero basta conoscere $T(v_1), ..., T(v_n) \in W$ per conoscere tutta la trasformazione lineare T.

Dimostrazione Se conosco T su $v_1, ..., v_n$ allora v si scrive come $v = \alpha_1 v_1 + ... + \alpha_n v_n$ (perchè $\mathcal{B} = \{v_1, ..., v_n\}$ genera v). T è lineare:

$$T(v) = T(\alpha_1 v_1 + ... + \alpha_n v_n) = \alpha_1 T(v_1) + ... + \alpha_n T(v_n)$$

Questo determina univocamente T:
Devo dimostrare che se esiste un'altra applicazione lineare $S \neq T$ ma che coincide con T sulla base, allora ho una contraddizione. Sia S un'altra applicazione $S : V \to W$ con $T(v_i) = S(v_i)$ $\forall i = 1, ..., n$ allora

$$S(v) = \alpha_1 S(v_1) + ... + \alpha_n S(v_n) = \alpha_1 T(v_1) + ... + \alpha_n T(v_n) = T(v)$$

T è determinata completamente dai suoi valori su una base B di V.

13.8 Corollario

Due applicazioni lineari coincidono $\Leftrightarrow$ coincidono sui vettori di una base.

13.9 Corollario

Se $\mathcal{B} = (v_1, ..., v_n)$ base ordinata di V e se $T : V \to W$ lineare, allora $ImT = Span(\{T(v_1), ..., T(v_n)\})$: cioè i vettori immagine della base di V generano l'immagine della trasformazione.

In particolare, se $T = L_A$, trasformazione lineare associata ad $A = \begin{bmatrix} a_{11} & .. & \\ & ... & \\ & .. & a_{mn} \end{bmatrix}$

$$T : \mathbb{R}^n \to \mathbb{R}^m$$

$$X \to AX = T(x)$$

allora

$$\begin{aligned} ImT = Im(L_A) &= Span(T(e_1), ..., T(e_n)) \\ &= Span(A \cdot e_1, A \cdot e_2, ..., A \cdot e_n) \end{aligned}$$

dove

$$A \cdot e_i = A \cdot \begin{bmatrix} 0 \\ \vdots \\ i \\ \vdots \\ 0 \end{bmatrix} = A^{(i)}$$

(Quindi questo punto del corollario ci dice che $Im(L_A) = Span(Colonne\ di\ A)$

$dimIm(L_A) =$ dimensione spazio generato dalle colonne
=numero dei pivot di una ridotta scala equivalente ad A)

13.10 Definizione: rango trasformazione lineare

1. Il rango di una trasformazione lineare $T : V \to W$ è $rg(T) = dim_K Im(T)$.
2. Il rango di L_A è la dimensione dell'immagine di L_A, che è il rango della matrice A, $ImL_A = \{AX : X \in \mathbb{R}^n\}$.

13.11 Teorema della dimensione

Sia $T : V \to W$ trasformazione lineare. Allora:

$$dimV = dim_K KerT + dim_K ImT$$

Sia $\{u_1, ..., u_s\} \subseteq V$ una base di $KerT$

- Generano $KerT$

- Sono indipendenti
- $T(u_1) = ... = T(u_s) = 0$

Per il teorema del completamento: completo $\{u_1, ..., u_s\}$ ad una base di V, quindi sia $\{u_1, ..., u_s, w_1, ..., w_{n-s}\}$ base di V. Si candidano a base di W i vettori $\{w_1, ..., w_{n-s}\}$.
Dobbiamo mostrare che $t = \{T(w_1), ..., T(w_{n-s})\}$ è una base di ImT, cioè che $rgT = n - s = dimV - dimKerT$

1. t genera $Im(T)$: sappieamo (dal corollario) che l'immagine ImT è lo span di $(T(u_1), T(u_2), ..., T(u_s), T(w_1), ..., T(w_{n-s})) = Span(0_w, T(w_1), ..., T(w_{n-s}))$

2. Vediamo che $T(w_1), ..., T(w_{n-s})$ sono indipendenti.
   Supponiamo $\alpha_1, ..., \alpha_{n-s} \in \mathbb{R}$ tali che:

$$\alpha_1 T(w_1) + ... + \alpha_{n-s} T(w_{n-s}) = 0$$

$$\Leftrightarrow T(\alpha_1 w_1 + ... + \alpha_{n-s} w_{n-s}) = 0 \ \ (T\ e'\ lineare)$$

$$\Leftrightarrow \alpha_1 w_1 + ... + \alpha_{n-s} w_{n-s} \in KerT$$

$$\Rightarrow \beta_1, ..., \beta_s : \ \alpha_1 w_1 + ... + \alpha_{n-s} w_{n-s} = \beta_1 u_1 + ... + \beta_s u_s$$

$$\alpha_1 w_1 + ... + \alpha_{n-s} w_{n-s} - \beta_1 u_1 - ... - \beta_s u_s = 0$$

   ed è una combinazione lineare dei vettori di una base di V che dà 0

$$\Rightarrow \alpha_1 = \alpha_2 = ... = \alpha_{n-s} = -\beta_1 = ... = -\beta_s = 0$$

13.12 Osservazione

Se $v_1, ..., v_n$ sono i vettori colonna di $\mathbb{R}^n$; sia $A = \begin{bmatrix} v_1 & v_2 & \dots & v_n \end{bmatrix}$ la matrice $m \times n$ formata dai vettori.
Allora una combinazione lineare delle colonne $v_1, ..., v_n$ con gli scalari $\alpha_1, ..., \alpha_n$ $(\alpha_1 v_1 + ... + \alpha_n v_n)$ è la stessa cosa di:

$$A_{(m \times n)} \cdot \begin{bmatrix} \alpha_1 \\ \cdots \\ \alpha_n \end{bmatrix} \in \mathbb{R}^m$$

13.13 Proposizione

a) $S, T : V \to W$, S, T lineari, V, W spazi vettoriali allora: $S + T$, $\lambda \cdot S$ sono lineari.
   Dove $(S + T)(v) := S(v) + T(v) : \forall v \in V \ \ (S + T : V \to W)$
   e dove $(\lambda S)(v) := \lambda S(v) \ \ (\lambda S : V \to W)$

b) Siano $S : U \to V$, $T : V \to W$ allora è possibile definire la composta $T \circ S : U \to W$, e $T \circ S$ è lineare.

Dimostrazione punto b) (la a) per esercizio)
Da dimostrare: $T \circ S$ è lineare $\Leftrightarrow T \circ S(\alpha v_1 + \beta v_2) = \alpha(T \circ S)(v_1) + \beta(T \circ S)(v_2)$

$$(T \circ S)(\alpha v_1 + \beta v_2) = T(S(\alpha v_1 + \beta v_2)) =$$

$$T(\alpha S(v_1) + \beta S(v_2)) = \quad \text{(S è lineare)}$$

$$\alpha T(S(v_1)) + \beta T(S(v_2)) = \quad \text{(T è lineare)}$$

$$\alpha(T \circ S)(v_1) + \beta(T \circ S)(v_2)$$

$$\Rightarrow T \circ S \text{ è lineare}$$

13.14 Conseguenze della proposizione

a) L'insieme $\mathcal{L}(V, W) = \{T : V \to W, T \text{ lineare}\}$ è uno spazio vettoriale

b) $\mathcal{L}(V, V)$ l'insieme delle trasformazioni lineari da V in se

$$T : V \to V \qquad T \circ S$$

$$S : V \to V \qquad S \circ T$$

$(\mathcal{L}(V, V), +, \cdot)$

- è un anello non commutativo
- unitario $id : V \to V$, $T \cdot id = id \cdot T = T$ (elemento neutro è l'unità del prodotto)
- $0_V : V \to V$ $(v \mapsto 0_V)$ trasformazione lineare nulla (elemeno neutro della somma)

c) Se in $\mathcal{L}(V, V)$ ci restringiamo a guardare le trasformazioni invertibili: $(\{T : V \to V : T \text{ lineare e invertibile}\}, \cdot)$ è un gruppo commutativo.

13.15 Osservazione: iniettività, suriettività

Sia $T : V \to W$ lineare e $dimV = dimW$, allora:

- T invertibile $\Leftrightarrow T$ iniettiva
- T invertibile $\Leftrightarrow T$ suriettiva

13.16 Osservazione: isomorfismo

V e W sono isomorfi (**notazione**: $V \cong W$) $\Leftrightarrow \exists\, T : V \to W$ con T biunivoca.

13.17 Esempio isomorfismo

V dimensione finita n; $B = (v_1, ..., v_n)$ base ordinata.

$$f_B : V \to \mathbb{R}^n$$

$$v \mapsto f_B(v) = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \text{ dove } v = x_1 v_1 + ... + x_n v_n$$

$f_B(v)$ sono le coordinate di v in base B. Si ha che f_B è un isomorfismo di V in $\mathbb{R}^n$.

L'isomorfismo $V \xrightarrow{f_B} \mathbb{R}^n$ non è canonico, cioè dipende dalla scelta di una base.

Conseguenza importante: tutti gli spazi vettoriali di dimensione n su K sono tutti isomorfi a K^n.

13.18 Teorema

$$\mathcal{L}(\mathbb{R}^n, \mathbb{R}^m) \cong \mathcal{M}_{m,n}(\mathbb{R})^{\to [m \cdot n]}$$

Dimostrazione: abbiamo visto già come associare ad una matrice $A_{m \times n}$ un'applicazione lineare di $\mathbb{R}^n$ in $\mathbb{R}^m$.
$A \mapsto L_A$ la trasformazione lineare da $\mathbb{R}^n$ in $\mathbb{R}^m$ che agisce per moltiplicazione.

$$L_A : \mathbb{R}^n \to \mathbb{R}^m$$

$$X \mapsto AX$$

$$L : Matrici\ m \times n \to \mathcal{L}(\mathbb{R}^n, \mathbb{R}^m)$$

$$A \mapsto L(A) = L_A$$

- L è biunivoca? C'è l'inversa?
- L è lineare? *Fare da soli*

Inizio dimostrazione primo punto:

$$L : \mathcal{M}_{m,n}(\mathbb{R}) \to \mathcal{L}(\mathbb{R}^n, \mathbb{R}^m)$$

$$A \leftarrow T$$

Ora

$$T : \mathbb{R}^n \to \mathbb{R}^m$$

$$e_1 \mapsto T(e_1) \in \mathbb{R}^m$$

$$\vdots$$

$$e_n \mapsto T(e_n) \in \mathbb{R}^m$$

Sia $A := \begin{bmatrix} T(e_1) & T(e_2) & \dots & T(e_n) \end{bmatrix}$ è una matrice $m \times n$.
Devo mostrare che $L_A = T$(*completare da soli!*)

13.19 Osservazione

Si può dimostrare che $L_A \cdot L_B = L_{A \cdot B}$

13.20 Proposizione: ricapitolazione sulle matrici invertibili

Le seguenti sono equivalenti:

1. $A \in \mathcal{M}_{m,n}(\mathbb{R})$ è invertibile (rispetto al prodotto di matrici)
2. $L_A : \mathbb{R}^n \to \mathbb{R}^n$ è invertibile
3. L_A è iniettiva
4. L_A è suriettiva
5. $KerA = \{0\}$
6. $ImL_A = \mathbb{R}^n$ $(= ImA)$
7. $rgA = n$
8. Le colonne di A sono indipendenti
9. Le righe di A sono indipendenti
10. $AX = \underline{0}$ ha l'unica soluzione $X = \underline{0}$
11. $\forall \underline{b} \in \mathbb{R}^n$ il sistema $AX = \underline{b}$ ammette unica soluzione (è $X = A^{-1} \cdot \underline{b}$)
12. I pivot di una ridotta scala sono tutti non nulli
13. $\exists\ B \in \mathcal{M}_n(\mathbb{R}) : BA = I_n = \begin{bmatrix} 1 & \dots & 0 \\ & \dots & \\ 0 & \dots & 1 \end{bmatrix}$ (*tutti 1 sulla diagonale, resto 0*)
    [inversa a sinistra]
14. $\exists\ C \in \mathcal{M}_n(\mathbb{R}) : AC = I_n = \begin{bmatrix} 1 & \dots & 0 \\ & \dots & \\ 0 & \dots & 1 \end{bmatrix}$ (*tutti 1 sulla diagonale, resto 0*)
15. $[A|I] \sim [I|C]$ (C^{-1} sarà l'inversa)
16. $det(A) \neq 0$

13.21 Determinante di una matrice quadrata

$$det : \mathcal{M}_n(\mathbb{R}) \to \mathbb{R}$$

$$A \mapsto det(A) \quad \text{(è un numero)}$$

13.21.1 Sistemi $AX = \underline{0}$

A è invertibile $\Leftrightarrow AX = \underline{0}$ ha unica soluzione.

13.21.2 $n = 1$

$A = [a]\ a \in \mathbb{R};\ X = x;\ \underline{0} = 0.$
$ax = 0$ ha unica soluzione $\Leftrightarrow a \neq 0 \Leftrightarrow a^{-1}ax = a^{-1}0\ (x = 0)$
(se $a = 0 : 0 \cdot x = 0$ ha infinite soluzioni). Qui se pongo $det(a) = a$ ottengo:

$$[a] = A \text{ invertibile} \Leftrightarrow det(A) = a \neq 0$$

TODO: CONTROLLARE SUL LIBRO

13.21.3 $n = 2$

A invertibile $\Leftrightarrow$ $AX = \underline{0}$ ha unica soluzione $\Leftrightarrow$ $a_{11}a_{22} - a_{12}a_{22} \neq 0$. *Dimostrazione su appunti lezione 33.*
Definisco:

$$detA = det \begin{bmatrix} a_{11} & a_{22} \\ a_{21} & a_{22} = \end{bmatrix} = a_{11}a_{22} - a_{21}a_{22}$$

13.21.4 $n = 3$

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

$$\text{det(A)=} \begin{array}{r|l|c} a_{11}\ a_{22}\ a_{33}+ & \left(\begin{smallmatrix}1&2&3\\1&2&3\end{smallmatrix}\right) = (1)(2)(3) & \text{segno pari} \\ a_{12}\ a_{23}\ a_{31}+ & \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right) = (123) & \varepsilon(\sigma) = 1 \\ a_{13}\ a_{21}\ a_{32}+ & \left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right) = (132) & \\ \cline{2-3} -a_{13}\ a_{22}\ a_{31} & \left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right) = (13) & \text{segno dispari} \\ -a_{11}\ a_{23}\ a_{32} & \left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right) = (23) & \varepsilon(\sigma) = -1 \\ -a_{12}\ a_{21}\ a_{33} & \left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right) = (12) & \end{array}$$

13.21.5 Definizione determinante

Data $A \in M_n(\mathbb{R})$, si definisce il determinante di A come:

$$detA = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1(\sigma 1)} a_{2(\sigma 2)} ... a_{n(\sigma n)}$$

NOTA: Esempio di matrice di permutazionee su slides lezione 34.

13.21.6 Proprietà del determinante

- $detA = detA^t$
- Se A ha una colonna tutta nulla, allora $detA = 0$ $(A^{(1)}\ A^{(2)}...\underline{0}...A^{(n)})$ colonne dipendenti.
- Se A ha una riga nulla allora il $detA = 0$ $(detA = detA^t)$.
- Se due colonne di A sono uguali, allora $detA = 0$.
- Se dure righe di A sono uguali, allora $detA = 0$.
- Se due colonne (risp. righe) sono proporzionali, cioè se $A = [A^{(1)}...A^{(i)}...\lambda A^{(i)}...A^{(n)}]$ allora $detA = 0$ ($\lambda A^{(i)}$ è la colonna j).
- Il valore del determinante non cambia se sommiamo ad una riga (vale anche l'analogo per le colonne) il multiplo di un'altra:

$$A = \begin{bmatrix} A_{(1)} \\ \vdots \\ A_{(i)} \\ \vdots A_{(n)} \end{bmatrix} \xrightarrow[L_{ij}(\lambda)]{} B = \begin{bmatrix} A_{(1)} \\ \vdots \\ A_{(i)} + A_{(j)} \\ \vdots \\ A_{(n)} \end{bmatrix}$$

  allora $det(A) = det(B)$.

- Se in A si scambiano due colonne (o due righe)

$$A = \begin{bmatrix} A_{(1)} \\ \vdots \\ A_{(i)} \\ \vdots \\ A_{(j)} \\ \vdots \\ A_{(n)} \end{bmatrix} \xrightarrow{L_{ij}} B = \begin{bmatrix} A_{(1)} \\ \vdots \\ A_{(j)} \\ \vdots \\ A_{(i)} \\ \vdots \\ A_{(n)} \end{bmatrix}$$

  allora $detA = -detB$.

13.21.7 Teorema di Binet

Siano A, B matrici quadrate $n \times n$ allora:

$$det(A \cdot B) = det(A) \cdot det(B)$$

(cioè il determinante è una funzione moltiplicativa sulle matrici).

!! non è additiva: $det(A + B) \neq det(A) + det(B)$

13.21.8 Corollario di Binet

$$det(A^{-1}) = \frac{1}{det(A)}$$

se A è invertibile.

13.21.9 Teorema di Lapalce

Calcolo del determinate col metodo di Laplace.

Data A $n \times n$, $n \geq 2$, si ha che (sviluppo lungo la colonna j quindi $A^{(j)}$):

$$\begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{nj} \end{bmatrix}$$

$$detA = a_{1j}\alpha_{1j} + a_{2j}\alpha_{2j} + ... + a_{nj}\alpha_{nj}$$

dove α_{ij} si chiama cofattore della matrice A, ed è definito come:

$$\alpha_{ij}(-1)^{i+j} \cdot detA_{ij}$$

A_{ij}: sottomatrice di A che si ottiene cancellando la riga i e la colonna j

1. ovvero: (formula per la colonna j)

   $$det(A) = \sum_{i=1}^{n}(-1)^{i+j} a_{ij} det(A_{ij})$$

   i: varia l'indice di riga; j è fisso.

2. formula (sviluppo) lungo la riga i

   $$det(A) = \sum_{j=1}^{n}(-1)^{i+j} a_{ij} det(A_{ij})$$

   j: varia l'indice di colonna; i è fisso.

NOTA: vedere appunti lezione 14 per esempio.

13.21.10 Metodo alternativo calcolo determinante

$A \sim B$ usando solo $L_{ik}, L_{ij}(C)$

$A \xrightarrow{L_{ij}} A'$: $detA = -detA'$ ($(-1)\cdot$ numero di scambi di riga)

$A \xrightarrow{L_{ij}(C)} A'$: $detA = detA'$

Non usare $L_i(C)$ perche modifica il determinante.

$$A = \begin{bmatrix} & & & \\ & & & \\ & & & \\ & & & \end{bmatrix} \sim B = \begin{bmatrix} b_{11} & & & \\ & b_{22} & & \\ & & b_{33} & \\ & & & b_{44} \end{bmatrix}$$

Il $detB$ = prodotto degli elementi sulla diagonale.

Proprietà: Se una matrice B quadrata è triangolare superiore (cioè $b_{ij} = 0$ se $i > j$)

$$\begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ 0 & b_{22} & \dots & b_{2n} \\ 0 & 0 & \dots & \\ 0 & \dots & 0 & b_{nn} \end{bmatrix}$$

allora $detB = b_{11}b_{22}...b_{nn}$ (prodotto degli elementi sulla diagonale.

- In particolare se b è una matrice diagonale, ovvero $b_{ij} = 0$ se $i \neq j$, allora $detA = b_{11}b_{22}...b_{nn}$
- In particolare se

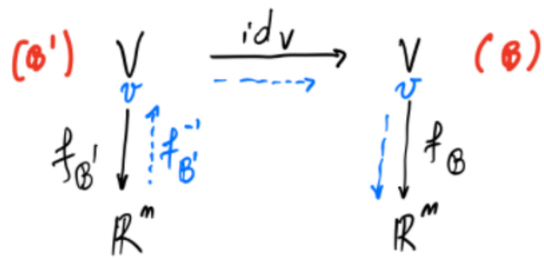
  $$B = \begin{bmatrix} \lambda & & \Huge 0 \\ & \lambda & \\ & \dots & \\ \Huge 0 & & \lambda \end{bmatrix} \text{ per } \lambda \in \mathbb{R}$$

  Allora $detB = \lambda^n$.
- $detI_n = \begin{bmatrix} 1 & & \Huge 0 \\ & \dots & \\ \Huge 0 & & 1 \end{bmatrix} = 1$ (Se a matrice ha tutti 1 sulla diagonale).
- Se P è una matrice di permutazione, allora $detP = \varepsilon(\sigma)$ se $P = P_\sigma$: P_σ è la matrice che ha 1 in posizione a_{ij} se $j = \sigma(i)$ NOTA: Esempio appunti lezione 34.

13.22 Cambiamento di base

- Come mutano le coordinate dei vettori nelle due basi diverse.
- Come mutano le trasformazioni lineari.
- Come cambiano le matrici associate alle trasformazioni quando cambiano le basi.

Siano $\mathcal{B} = (v_1, ..., v_n)$ e $\mathcal{B}' = (v'_1, ..., v'_n)$ due basi ordinate di uno spazio vettoriale V (su $\mathbb{R}$ o su K fissato) di dimensione n su $\mathbb{R}$ (su K...). Siano $f_{\mathcal{B}}$ ed $f_{\mathcal{B}'}$ gli isomorfismi che mandano i vettori di V nelle coordinate (colonne di $\mathbb{R}^n$) rispettivamente nella base $\mathcal{B}$ e $\mathcal{B}'$.



$$id_V : V \to V$$

$$v \mapsto v = id_V(v)$$

(id_V è una trasformazione lineare biunivoca) è l'elemento neutro nella composizione delle trasf.lineari da V in se.

Richiamo Se $\mathcal{B}$ è una base, allora l'applicazione

$$f_{\mathcal{B}} : V \to \mathbb{R}$$

$$v \to \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

Se $v = x_1 v_1 + ... + x_n v_n$, $\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = f_{\mathcal{B}(v)}$ è

- Lineare
- Biunivoca

14 Usi di Gauss-Jordan in vari ambiti

14.1 Risolvere $AX = b$

Si applica GJ alla matrice aumentata $[A|b] \to [R|b']$ con $A \sim R$ e $[A|b] \sim [R|b']$.

$AX = b$ ha le stesse soluzioni di $RX = b'$. Si risolve a questo punto il sistema ridotto $RX = b'$

14.2 Rango e base ImL_A

Si applica $A \to R$.

Rivedere Corollario ImL_A

Le colonne sono generatori:

$$[A^{(1)}, ..., A^{(n)}] = A \sim R$$

allora le colonne di A corrispondenti ai pivot sono indipendenti: $A^{(j_1)}...A^{(j_r)}$:

$$rg(A) = dimImL_A = r$$

e $A^{(j_1)}...A^{(j_r)}$ è una base per l'immagine.

14.3 Trovare $Ker(L_A) = KerA$

$$KerT = \{v \in V : T(v) = 0\}$$
$$KerL_A = \{X \in \mathbb{R}^n : L_A(X) = \underline{0}\} =$$
$$\{X \in \mathbb{R}^n : AX = \underline{0}\} =$$

$=$ spazio delle soluzioni del sistema lineare omogeneo associato ad A

$KerA$ =Soluzioni di $AX = 0$: applicando GJ ad A: $A \sim R$ e risolvo ora $RX = 0$.

14.4 Estrazione insieme di vettori indipendenti

Per il problema di estrarre un insieme indipendente più grande possibile da un insieme di vettori di $\mathbb{R}^n$: ci si chiede dato $\{v_1, ...v_k\} \subseteq \mathbb{R}^n$, qual è una base per $Span(v_1, ..., v_n)$ da estrarre da $\{v_1, ...v_k\}$.
Costruisco la matrice $A = \begin{bmatrix} v_1 & \dots & v_k \end{bmatrix}_{nxk}$:
$A \sim^{GJ} R$: le colonne di A corrispondenti alle colonne di R dove si trovano i pivot sono indipendenti.

14.5 Completamento a un base di $\mathbb{R}$

Dati $v_1, ..., v_k \in \mathbb{R}^n$ indipendenti, voglio completare $\{v_1, ..., v_k\}$ a una base di $\mathbb{R}^n$ (se $k < n$).

In questo caso formo un insieme $\{v_1, ..., v_k, e_1, ..., e_n\}$. Costruisco

$$A = \begin{bmatrix} v_1 & \dots & v_k & e_1 & \dots & e_n \end{bmatrix}$$

Applico GJ: $A \sim R$ e scelgo le colonne di A corrispondenti ai pivot.

14.6 Trovare base di $U + W$ e $U \cap W$

Per trovare una base di $U + W$ e $U \cap W$ date una base di U e una di W.