Matematica discreta algebra geometría	Argomento trattato:
Lezione mercoledì 19/09/2024	Insiemistica (Matematica Discreta) prof.Yu Chen

Domande e risposte / parole chiave

-Insieme
-Elementi

-Ben definita: gli elementi sono determinabili se appartengono o no all'insieme

Z={numeri interi}
Q={numeri razionali}
C={numeri complessi}
R={numeri reali}

Simboli:
|= tale che
$\in$ = appartenente
$\notin$= non appartenente
{}=simbolo di insieme
$\subseteq$ = inclusione
/$\subseteq$ = non inclusione
$\Leftrightarrow$ = se e solo se
$\varnothing$ = vuoto

Appunti:
Definizione di insieme: è una collezione ben definita di oggetti (detti elementi dell'insieme)

Come descrivere un insieme:

1) Con un elenco completo degli elementi dell'insieme
   Es. A={1,3,5}
   Es. B={0,1{0,1}} è uguale a scrivere →{0,1,X} se X={0,1} (in questo caso {0,1} è un elemento) Y={{0,1}}={X}

---

2) Dando un criterio per gli elementi
   Es. A={studenti di informatica}
   Es. X={radici dell' equazione x^2 -1=0}={1,-1}

---

3) Se un elemento x appartiene ad un insieme A
   si scrive:x $\in$ A
   al contrario quando un elemento x non appartiene all'insieme
   Si scrive:x $\notin$ A
   Sia P una proprietà/affermazione
   Per x $\in$ A , P(x) rappresenta→ x soddisfa P
   A={x|P(x)} (significa che A è uguale all' insieme in cui ci sia x tale che soddisfi la proprietà)

   Es. X={x | x^2 -1=0} (si può anche scrivere X={x : x^2 -1=0}
   Es. N={x $\in$ Z | x>=0}

Definizione di cardinalità: la cardinalità di un insieme A ,|A|,
È il numero degli elementi in A
|A|<∞⟶(cardinalità finita) |A|=∞⟶(cardinalità infinita)
Es. |{0,1}| = 2(cardinalità(ho 2 elementi))
Es. |{{0,1}}| = 1
Es. |N| = ∞
Es. |$\varnothing$|=0 , |{$\varnothing$}|=1

Definizione di sottoinsieme : un insieme B è un sottoinsieme si un insieme A se ogni elemento B è anche un elemento di A
Si scrive: B$\subseteq$A
Al contrario: B /$\subseteq$ A

	Es. $N \subseteq Z \subseteq Q \subseteq R \subseteq C$ Es. sia A un insieme allora x(elemento) $\in$ A(insieme) $\Leftrightarrow$ {x} $\subseteq$ A --- Definizione di insieme vuoto: un insieme vuoto($\varnothing$) è un insieme privo di elementi $\varnothing \subseteq$ A (ogni insieme è sottoinsieme di se stesso) --- Definizione insiemi uguali: due insiemi A e B sono detti uguali se e solo se A è sottoinsieme di e B è sottoinsieme di A ($A \subseteq B$ E $B \subseteq A$) Es. sia A insieme di B={A,{A}} Si ha : $A \in B$, $\{A\} \in B$, $\{A\} \subseteq B$,
RIASSUNTO:	Scrivi qui il tuo riassunto:

Matematica discreta algebra geometría	Argomento trattato:
Lezione venerdì 20/09/2024	Matematica discreta (Prof yu chen) sottoinsiemi e operazioni degli insiemi
Domande e risposte / parole chiave Simboli: -P()=Insieme delle parti	Appunti: Def. insieme delle parti: si dice insieme delle parti un insieme in cui gli elementi siano i sottoinsiemi di un insieme Es. sia A un insieme il suo insieme delle parti sarà: $P(A):=\{x \mid x \subseteq A\}$

-":=" = definiamo
|= tale che
∈= appartenente
∉= non appartenente
{}=simbolo di insieme
⊆= inclusione
/⊆ = non inclusione
⇔ = se e solo se
∅ = vuoto
|A|=cardinalità
∩ = interseca
∪= unione
C_X=complemento

Come trovare tutti i sottoinsiemi di un insieme:
1)ogni elemento è un sottoinsieme dell'insieme
Es. A={a,b}→P(A)={∅,{a},{b},{a,b}
2)ogni insieme può essere considerato come suo sottoinsieme

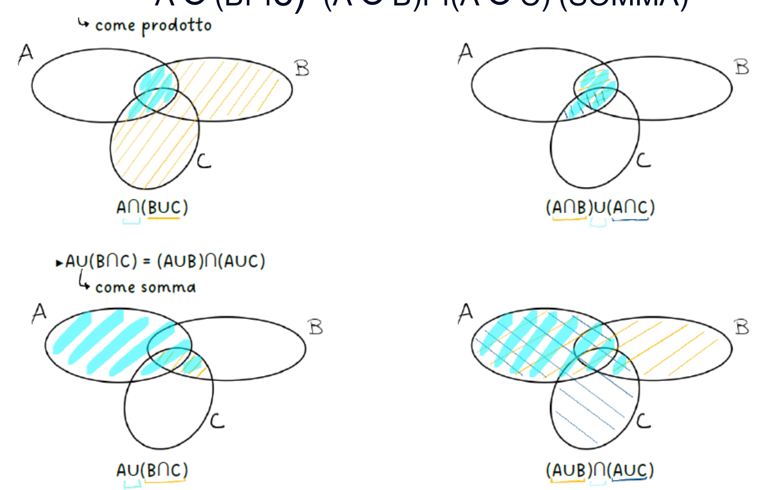
Proprietà di cardinalità dei sotto insiemi
Se |A|=n allora → $P(A)=2^n$
Es. dati A e B insiemi allora A=B ⇔ P(A)=P(B) (A e B sono uguali se e solo se i loro insiemi delle parti sono uguali.

1) Def. l'intersezione tra A e B si scrive: A∩B :={X|X∈A e X∈B}
   es.A={1,2,3} B={3,4,5} C{4,5}
   A∩B={3} A∩C =∅
   A e B sono disgiunti se A∩B=∅
2) L'unione di A e B si scrive A∪B :={X|X∈A oppure X∈B}
   Es. A∪B={1,2,3,4,5} A∪C={1,2,3,4,5}
   Quando abbiamo più intersezioni o unioni :
   es . siano A_1, A_2……. ,A_n insiemi scriviamo:

$$\bigcap^{n} A_i=A_1\cap A_2\cap\ldots\cap A_n$$ in caso siano intersezioni

$$\bigcup^{n} A_i=A_1\cup A_2\cup\ldots\cup A_n$$ in caso siano unioni

Proprietà delle intersezioni e delle unioni
1) Associatività: (A∩B)∩C=A∩(B∩C) , (A∪B)∪C=A∪(B∪C)
2) Idempotente: A∩A=A,A∩∅=∅ , A∪A=A,A∪∅=A
3) Distributività: A∩(B∪C)=(A∩B)∪(A∪C)(PRODOTTO)
   A∪(B∩C)=(A∪B)∩(A∪C) (SOMMA)

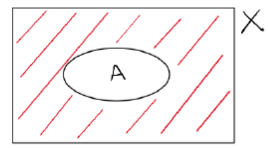


Def. di complemento : sia A un sottoinsieme di X il complemento di A in X sarà (ovvero un insieme complementare):
C_X(A):={X∈X|X∉A} (si può scrivere anche Ā)

Def. Sia A un sottoinsieme di X. Si dice complemento (insieme complementare) di A in X e si denota $C_X(A)$ il sottoinsieme degli elementi di X non in A

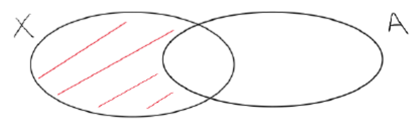
$C_X(A) := \{x \in X \mid x \notin A\}$

$\hookrightarrow = \bar{A}$



Def. di differenza : dati 2 insiemi A e X, la differenza tra X ed A è un sottoinsieme di X , si scrive : $X-A:=\{X \in X|X \in A\}$ (può essere scritto anche $X \setminus A:=\{X \in X|X \in A\}$

Def. Dati insiemi A e X, la differenza di X e A è un sottoinsieme di X: $X-A := \{x \in X \mid x \notin A\} \rightarrow X \setminus A$



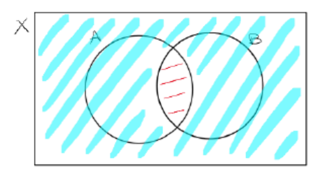
Teorema di de morgan: sia A e B 2 sottoinsiemi di X:

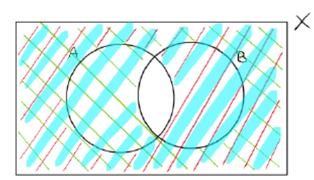
$C_X(A \cap B)=C_X(A) \cup C_X(B)$ (stessa cosa $A \cap B=\bar{A}\,\overline{\cup}\,\mathbf{B}$)

Teorema: De Morgan, Sia A e B sottoinsiemi di un X:

▸ $C_X(A \cap B) = C_X(A) \cup C_X(B)$

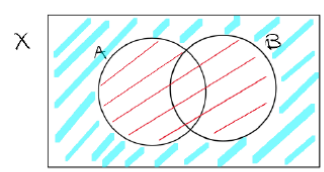
cioè $\overline{A \cap B} = \bar{A} \cup \bar{B}$

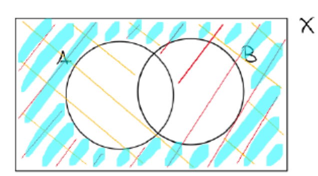




▸ $C_X(A \cup B) = C_X(A) \cap C_X(B)$

cioè $\overline{A \cup B} = \bar{A} \cap \bar{B}$





$C_X(A \cup B)=C_X(A) \cap C_X(B)$ (stessa cosa $A \cup B=\bar{A}\,\overline{\cap}\,\mathbf{B}$)

1)def. Di ricoprimento: Siano $A_1, A_2 \ldots\ldots , A_n$ sottoinsiemi di un insieme A

$\{A_i\}_{i=1}:=\{A_1, A_2 \ldots\ldots ,A_n\}$ è un ricoprimento di A se $\cup$ di n $Ai=A_1 \cup ,A_2 \cup \ldots\ldots ,A_n$

Es. A=Z , A_1={numeri interi pari } A_2={numeri interi dispari}

$A= A_1 \cup A_2$

$\{A_1,A_2\}$ ricoprimento di A

Es. $A=\{1,2,3,4,5\}$ $A_1=\{1,2,3\}$ $A_2=\{3,4,5\}$ $A_3=\{4,5\}$

$A= A_1 \cup A_2 = A_1 \cup A_2 \cup A_3$ ⇨ $\{A_1,A_2\}$ ricoprimento di A $\{A_1,A_2,A_3\}$

2)def. Di partizione: $\{A_i\}^n_{i=1}$ è una partizione di A se:

1) $\{A_i\}^n_{i=1}$ è un ricoprimento

2) $A_i \neq 0$, i=1,2,....,n

	3) $A_i \cap A_j = \varnothing$ per tutti gli i i<=n e 1<=j<=n i $\neq$j (la partizione è un insieme delle parti vuoto) Es. A_1={numeri interi pari } A_2={numeri interi dispari} Z=$A_1 \cup A_2$, $A_1 \cap A_2 = \varnothing$ ⇨ {A_1,A_2} è ripartizione di Z Es. {A_1,A_3} è ripartizione di A Perchè: 1) A $\cup$ A_3=A 2) $A_i \neq \varnothing$ 3) $A_i \cap A_3 = \varnothing$
RIASSUNTO:	Scrivi qui il tuo riassunto:

Matematica discreta algebra geometría	Argomento trattato:
Lezione mercoledì 24/09/2024	(matematica discreta) prof. Yu chen
Domande e risposte / parole chiave Simboli: -P()=Insieme delle parti	Appunti: Def. prodotto cartesiano: dati A,B due insiemi: un prodotto cartesiano di A e B è un insieme AxB:={a,b)| $\forall$ a $\in$ A , $\forall$ b $\in$ B} Es. A={1,2,3}, B={2,4}

-":=" = definiamo
|= tale che
$\in$= appartenente
$\notin$= non appartenente
{}=simbolo di insieme
$\subseteq$= inclusione
/$\subseteq$ = non inclusione
$\Leftrightarrow$ = se e solo se
$\varnothing$ = vuoto
|A|=cardinalità
$\cap$ = interseca
$\cup$ = unione
C_X=complemento

[ ]= intervallo
R=relazione
~~= è in relazione
Γ=gamma
∃= esiste

AxB:={(1,2),(1,4),(2,2),(2,4),(3,2),(3,4)}
AxB={(1,2),(1,4),(2,2),(2,4),(3,2),(3,4)}
Es. A=[0,1]:={x$\in$R|0<=1}$\subseteq$R
B=[-1,0]:={y$\in$R|-1<=y<=0}$\subseteq$R

Inserire piano cartesiano

AxB={(x,y)|$\forall$0<=x<=1,$\forall$-1<=y<=0
Def. relazione tra 2 insiemi: dati AeB insiemi non vuoti una relazione tra A e B è un sottoinsieme: R$\subseteq$AxB
Es. A={1,2,3} B={3,4,5}
R_1={(1,3),(2,4),(3,3)}$\subseteq$AxB
R_2={(1,3),(1,4)}$\subseteq$AxB
Es. A=B R$\subseteq$AxA (R quindi è una relazione di A (in A))
Per a,b$\in$A se (a,b) $\in$R $\subseteq$AxA
a è in relazione con b →(si scrive anche a~~b$\Leftrightarrow$(a,b)$\in$R
Proprietà delle relazioni:

1) R è riflessiva se per $\forall$a$\in$A a~~a
   Es. A={1,2,3,4}
   R={(1,1),(2,2),(3,3),(4,4)}$\subseteq$AxA
   R è riflessiva
   R^1={(1,2),(3,4)} non riflessiva
2) R è simmetrica se $\forall$a$\in$A , $\forall$a$\in$A
   Se a~~b allora b~~a ovvero se(a,b)$\in$R allora(b,a)$\in$R
3) R è transitiva se per a,b,c $\in$ A
   Se a~~b e b~~c allora a~~c
   Una relazione è equivalente se R è
   -riflessiva
   -simmetrica
   -transitiva

Proprietà: esiste una corrispondenza biunivoca tra le relazione di equivalenza insieme A e la partizione di A

Def. siano A e B insiemi non vuoti una funzione con dominio A e codominio B e un dato sottoinsieme di AxB
Γ$\subseteq$AxB tale che $\forall$a$\in$A esista un unico b$\in$B tale che (a,b)$\in$Γ
Es. A={1,2,3},B{2,4}
R={(1,2),(2,2),(3,4)}$\subseteq$AxB

R_1={(1,2),(1,4),(2,4)}$\subseteq$AxB
es.R={C_X,x^2+1)$\in$RxR|$\forall$x$\in$R}
$\subseteq$xR è la stessa cosa di scrivere f(x)x^2+1
Sia Γ $\subseteq$ AxB una funzione
Def. F: A→B
$\forall$a$\in$A,a→f(a)$\in$B
a$\in$A ⇒esiste(a,b) $\in$ Γ

	Si definisce f(a)=b f(A) è l'immagine di a $\Gamma \subseteq AxB$ Inserire diagramma di ven Per verificare che una corrispondenza sia una funzione: 1) ogni elemento di A deve avere un immagine in B (BEN DEFINITA) 2) ogni elemento di A ha una sola immagine in B (DEFINIZIONE DI FUNZIONE) propietà Se e solo se soddisfa entrambe una funzione è ben definita Es. $F:R\rightarrow R$, $\forall x \in R$, $F(x)=1/x \Leftrightarrow \Gamma=\{(x,1/x) \in RxR$ Non esiste F(0) cioè $0 \in R$ non ha alcuna immagine per ciò F non è una funzione. Es. F $R\setminus\{0\}\rightarrow R$, $\forall x \in R$, $x\rightarrow 1/x$ è una funzione (se valgono entrambi) 1) Def. sia $F:A\rightarrow B$ una funzione $\forall a \in A$, F(a) è immagine di a per $b \in B$ se $\exists a \in A$ tale che F(a)=b , a si chiama controimmagine di b 2) Sia $x \subseteq A$ $F(x) \subseteq B$ $F(x)=\{F(x)\mid \forall x \in x\}$ Immagine di x Sia $Y \subseteq B$ $F^{-1}(Y):=\{x \in A\mid F(x) \in$ yìY$\} \subseteq B$ Controimmagine di Y

RIASSUNTO:	Scrivi qui il tuo riassunto:

Matematica discreta algebra geometría	Argomento trattato:
Lezione giovedì 03/10/2024	(matematica discreta) prof. Yu chen
Domande e risposte / parole chiave Simboli: -P()=Insieme delle parti -“:=” = definiamo |= tale che $\in$= appartenente $\notin$= non appartenente {}=simbolo di insieme $\subseteq$= inclusione $\nsubseteq$ = non inclusione $\Leftrightarrow$ = se e solo se $\varnothing$ = vuoto |A|=cardinalità $\cap$ = interseca $\cup$= unione C_X=complemento $\Rightarrow$= allora [ ]= intervallo R=relazione (quella che non ho 😓) $\sim$= è in relazione Γ=gamma $\exists$= esiste $\subsetneq$=inclusione -insieme vuoto $\neq$=diverso	Appunti: Siano A e B 2 insiemi finiti non vuoti $\|A\|<\infty,\|B\|<\infty$ → cardinalità finta. Se $B\subseteq A\Rightarrow\|B\|<=\|A\|$ Sia $F:A\to B$ una funzione Allora: 1) $\|A\|>=\|F(A)\|$ $\|B\|>=\|F(A)\|$ 2) Se F suriettiva ossia $F(A)=B\Rightarrow\|A\|>=\|F(A)\|=\|B\|$ 3) Se F iniettiva: F:A(dominio)→F(A)$\subseteq$B(codominio) Questa funzione è biettiva perchè è sia suriettiva che iniettiva. Quando una funzione è biettiva la cardinalità dei due insiemi è la stessa $\Rightarrow\|A\|=\|F(A)\|<=\|B\|$ 4) F biettiva $\Rightarrow\|A\|=\|B\|$ Es. A,B insiemi finiti Allora: 1) $\|A\|>=\|B\|\Leftrightarrow$ se esiste una funzione $F:A\to B$ (surriettiva) 2) $\|A\|<=\|B\|\Leftrightarrow\exists\ F:A\to B$ (iniettiva) 3) $\|A\|=\|B\|\Leftrightarrow\exists F:A\to B$ (biettiva) Proprietà: sia A un insieme finito allora una funzione $F:A\to A$ è suriettiva se e solo se F è iniettiva --- Definiamo: due insiemi A e B sono equipollenti se: esiste una funzione biettiva $F:A\to B$ ossia A e B hanno la stessa cardinalità $\|A\|=\|B\|$ Se $\exists$ F:→B iniettiva si dice $\|A\|<=\|B\|$ Se $\exists$ F:→B suriettiva si dice $\|A\|>\|B\|$ Proprietà di A,B insiemi allora sono equipollenti se: $\|A\|=\|B\|$ (biettiva)$\Leftrightarrow\|A\|<=\|B\|$ (iniettiva) e $\|A\|>=\|B\|$ (suriettiva) Es. $F:N\to 2N=\{2n\|\forall n\in N\}\subsetneq N\ \ \forall n\in N,n\to 2n$ F è {ovunque definita ed è funzionale }$\Rightarrow$f è una funzione ben definita F è {iniettiva e suriettiva } allora f è biettiva $\Rightarrow\|N\|=\|2N\|\to$ solo su insiemi finiti. --- Un insieme A è infinito se e solo se è equipollente ad uno dei suoi sottoinsiemi propri. Es. $NxN=\{(a,b)\|\forall\ a,b\in N\}$

	Teorema: ogni insieme finito non vuoto è equipollente ad un insieme N dove n= alla cardinalità dell'insieme. (non metto la dimostrazione) $\|N \times N\|=\|N\|$ se la funzione è biettiva 2) per ogni insieme infinito x si ha $\|N\| \leq \|X\|$ --- Proprietà: se A,B sono insiemi finiti allora valgono le seguenti proprietà: 1) Se $B \subseteq A \Rightarrow \|A-B\| = \|A\|-\|B\|$ 2) Se $B \not\subset A \Rightarrow \|A-B\|=\|A\|-\|A \cap B\|$ 3) Se $A \cap B = \varnothing \Rightarrow \|A \cup B\|=\|A\|+\|B\|$ 4) Se $A \cap B = \varnothing \Rightarrow \|A \cup B\|=\|A\|+\|B\|-\|A \cap B\|$ 5) A,B,C finiti allora : $\|A \cup B \cup C\|=\|A\|+\|B\|+\|C\|-\|A \cap B\|$ Es. per un gruppo di studenti iscritto ad informatica di cui: M= 152 hanno superato md A= 144 hanno superato AG (speriamo di essere qui) $M \cap A$=89 hanno superato entrambi (si ciao non succede mai) Quanti sono gli studenti che hanno passato almeno un esame ? $M \cup A=\|M\|+\|A\|-\|M \cap A\|$ In termini numerici: 152+144-89 =207
RIASSUNTO:	Scrivi qui il tuo riassunto:

Matematica discreta algebra geometría	Argomento trattato:
Lezione 26/09/2024	Suriettività iniettività e biettività come influiscono sulla cardinalità (Matematica discreta) prof. Yu chen
Domande e risposte / parole chiave	Appunti:

Simboli:
-P()=Insieme delle parti
-“:=” = definiamo
|= tale che
$\in$= appartenente
$\notin$= non appartenente
{}=simbolo di insieme
$\subseteq$= inclusione
/$\subseteq$ = non inclusione
$\Leftrightarrow$ = se e solo se
$\varnothing$ = vuoto
|A|=cardinalità
$\cap$ = interseca
$\cup$= unione
C_X=complemento

[ ]= intervallo
R=relazione
$\sim$= è in relazione
Γ=gamma
∃= esiste
$\subsetneq$=inclusione -insieme vuoto
$\neq$=diverso

Definiamo la suriettività: una funzione $f:A\rightarrow B$ è suriettiva se ogni $b\in B$ ha una controimmagine
Ossia: $\forall b\in B$ avremo:
$|f^{-1}(b)|=|\{a\in A|f(a)=b\}|>=1$ (1 è la cardinalità dell' insieme l'insieme non è vuoto dato che la sua cardinalità è strettamente maggiore ad uno)
Es. $f:z\rightarrow Z$ $f(a)=a+1$
$\forall a\in Z$ $a\rightarrow a+1$

1) È ben definita (ogni elemento di Z ha un immagine in f)
2) È funzionale (ogni elemento di Z ha una sola immagine in f)
3) È suriettiva spieghiamo perchè:
   f è suriettiva perchè:
   $\forall x\in Z$ avremo un codominio$\rightarrow f(x-1)=(x-1)+1=x$
   Allora possiamo dire che x-1 è controimmagine di x (ovvero $x\in Z$ ha una controimmagine)
   Allora f è suriettiva perchè:
   $f^{-1}(x) = \{y\in Z|f(y)=x\}$
   $=\{x-1\}$
   $|f^{-1}(x)|=1$

Iniettiva: se ogni elemento di B è immagine di più di un elemento di A

$f:A\rightarrow B$ è iniettiva se $a1,a2\in A,a1\neq a2$
Allora $f(a1)\neq f(a2)$ $f:z\rightarrow Z$, $f(a)=a+1$
Es. di iniettività:
Per $a1\neq a2 \in Z$ (dominio)
$f(a1)=a1+1$, $f(a2)=a2+1$
Allora $a1+1\neq a2+1$
Allora $f(a1)\neq f(a2)+$
Questo dimostra l’iniettività di f
,

Esempio di suriettività
Es. $f:z\rightarrow Z$
$\forall a\in Z$ $a\rightarrow a^2+1\}f(a)=a^2+1$
f(z) (ovvero l’insieme delle immagini)
$f(z)=\{x\in Z|f(x)\}$
$= \{x\in Z|x^2+1\}\subsetneq Z$
Allora esiste $y\in Z$ tale che $f^{-1}(y) =\varnothing;y<0$
Allora f è suriettiva
Inserire schema
Per $a1,a2 \in Z$
$f(a1)=a1^2+1$, $f(a2)=a2^2+1$
Se $a1\neq a2$, se $a1=-a2$
Per $5\in Z$ codominio
$f(2)=2^2+1=5$
$f(-2)=5$
Allora possiamo dire che f non è iniettiva
$f^{-1}(5)=\{2,-2\}$
$1<|f^{-1}(5)|=2$
Def. una funzione $f: A\rightarrow b$ è biettiva se è suriettiva e iniettiva
A,b,c insiemi:
$f:A\rightarrow B$, $g:B\rightarrow C$
Inserisci diagramma di ven

Def. date $f:A\rightarrow B$, $g:B\rightarrow C$ funzioni : la composizione di f e g è una funzione: $g*f:A\rightarrow C$

	$\forall a \in A\ a \to g*f(a) := g(f(a))$ Es. $f:R\to R$ $\quad$ $g:R\to R$ $x\to f(x)=2x$ $\quad$ $x\to g(x)=x+1$ $\forall a \in R\ g*f(x)=g(f(x))=g(2x)=2x+1$ $f*g(x)=f(g(x)=f(x+1)=2(x+1)$ Attenzione! $f*g \neq g*f$ Proprietà: siano $f:A\to B$, $g:B\to C$, $h:C\to D$ Allora $h*(g*f)=(h*g)*f$ $\downarrow \quad \downarrow$ $A\to D \quad A\to D$ Es. siano $A\xrightarrow{f}B\xrightarrow{g}C$ 1) Se f e g sono suriettive: allora $g*f$ è suriettiva 2) Se f e g sono iniettive allora $g*f$ è ignettiva 3) Se $g*f$ è suriettiva allora f è suriettiva 4) Se $g*f$ è iniettiva allora g è iniettiva
RIASSUNTO:	Scrivi qui il tuo riassunto:

Matematica discreta algebra geometría	Argomento trattato:
Lezione mercoledì 17/10/2024	Permutazioni (matematica discreta) prof. Lea Terracini
Domande e risposte / parole chiave id = identità Sn=gruppo delle permutazioni sugli elementi	Appunti: Permutazioni: sono modi per riordinare gli elementi di un insieme X0{a,b,c} Potrà avere le seguenti combinazioni: abc acb bac bca cab cba Def. Sia $x\neq\emptyset$ una permutazione su x è una funzione biettiva $x\to x$ Es.

Se x ={a}
Se x=a l’unica permutazione su x è l'identità x→x a→a

Poniamo Sx={permutazioni su x}
|Sx|=1 se |x|=1
In generale id є Sx per ogni x≠Ø quindi Sx≠Ø
Se x ={a,b}
Sx={id, σ}
Dove σ x→x e t.c. σ(a)=bσ (b)=a

Se X è un insieme finito (|z|=n)
Allora |Sx|=n!

Date σ, т є Sx possiamo farne la composizione
σ*т : x→x

∀xєX σ*т(x) = σ(т(x))
Se σ,т є Sx anche σ*т є Sx

La composizione è un’ operazione su Sx
Un'operazione è una funzione del tipo:
Sx X Sx→Sx (σ,т)→σ*т
Proprietà della composizione:
-è assocciativa
Dati σ,Ƕ, ***v*** є Sx
σ*(Ƕ****v***)=(σ*Ƕ)****v***
-l’identità è l’elemento neutro
∀σєSx σ*id x = id x * σ =σ
-ogni elemento in Sx ha un inversa
se σєSx $σ^{-1}$єSx
La funzione inversa è $σ^{-1}$(a)=b t.c
σ(b)=a
Quindi $σ*σ^{-1}=σ^{-1}*σ$=id

Sx è un gruppo rispetto alla composizione.
In generale possiamo dire che la composizione non è commutativa se |x|>2
(c’è la dimostrazione ma non la scrivo)

Se x è un insieme finito e |x|=n possiamo supporre X=In={1,2….n}
In questo caso
Sin=Sn

Come rappresentare una permutazione
1)rappresentazione matriciale:
Es. se σ єS3 è definita da
σ(1)=1 σ(2)=3 σ(3)=2

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

In generale la rappresentazione matriciale di σ єSn è:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$$

Tutti gli elementi In compaiono 1 e un una sola volta
Es.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 1 \end{pmatrix}$$ non è biettiva per ciò non è una permutazione

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 3 \end{pmatrix}$$ è biettiva quindi ∈ S4

Come calcoliamo la composizione?
-composizione di permutazioni
Es.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix} \mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}$$

Procediamo a calcolarlo con una matrice d'appoggio

$$\begin{pmatrix} & 1 & 2 & 3 & 4 & 5 \\ \mu & 2 & 3 & 4 & 1 & 5 \\ \sigma & 1 & 5 & 4 & 2 & 3 \end{pmatrix}$$ procedo dalla matrice più esterna e riscrivo le immagini e faccio uguale per quella più interna in base alle immagini della precedente

$$\sigma \circ \mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 2 & 3 \end{pmatrix}$$

Ora invertiamo l'ordine degli addendi

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix} \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$$

$$\mu \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}$$ (ho usato lo stesso procedimento di prima)

Posso calcolare nello stesso modo $\sigma*\sigma=\sigma^2$ $\sigma*\sigma*\sigma=\sigma^3$ $\sigma^n=\sigma*......\sigma^n$
σ^0=identità

Inversa di σ

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$$

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$$

$\sigma^{-n}=(\sigma^{-1})^n=(\sigma^n)^{-1}$

es

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}$$

$$\tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 3 & 5 \end{pmatrix}$$ (regola generale leggere la prima riga e scrivere il numero precedente a quello che ci interessa es per 2 sarà 1

I cicli
Es. in S6

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 4 & 1 & 6 \end{pmatrix}$$ il suo ciclo sarà σ=(1 2 3 4 5)

Def: sia I={i1…….ik}⊆In con i1…ik distinti, k>=2 una permutazione tale che:
σ(i1)=i2
σ(i2)=i3
σ(i3)=i4
σ(ik-1)=ik
σ(ik)=ik
E σ(j)=j∉i
Si dice ciclo di lunghezza k o kciclo

Un 2 ciclo si dice scambio o trasposizione

Attenzione non tutte le permutazioni sono cicli:

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 3 & 1 & 5 & 7 & 2 \end{pmatrix}$$

1→4 2→6→7 NON è UN CICLO!!!
μ è prodotto di 2 cicli

La scrittura di un ciclo come stringa è invariante per permutazioni circolari.

L'inversa di un ciclo è un ciclo se σ0(i1 i2 i3 ….ik
σ^{-1}=(ik ik-1…….i3 i2 i1)
Es.
  $(3\ 1\ 4\ 2)^{-1}$ = (2 3 1 3)
  $(2\ 7)^{-1}$ = (7 2)
Osserviamo che gli scambi sono gli inversi di se stessi

Def. due cicli σ={i1…ik} μ=(i1….ik)
In Sn sono disgiunti se
{i1…..ik}∩{j1….jk}=Ø
Es.
  (1 3) (5 4 2) sono disgiunti
  (1 3)(5 4 1) non sono disgiunti
Proposizione:
Cicli disgiunti commutano
Cioè se σ, μ є Sn sono cicli disgiunti
Allora σ*μ=μ*σ

	(c'è una dimostrazione ma famo che non la scrivo)
RIASSUNTO:	Scrivi qui il tuo riassunto: Permutazioni: (Sn, *) gruppo Notazione matriciale $\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$ Cicli disgiunti {i1…..ik}∩{j1….jk}=Ø I cicli disgiunti commutano

Matematica discreta algebra geometría	Argomento trattato:
Lezione mercoledì 22/10/2024	(Matematica discreta) prof. Lea Terracini
Domande e risposte / parole chiave	Appunti: Ogni permutazione si scrive come prodotto di cicli disgiunti in modo unico. Es. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 5 & 1 & 6 & 2 & 3 & 9 & 8 & 7 \end{pmatrix}$ Può essere scritta come prodotti di cicli così: (1 4 6 3)(2 5)(7 9) (8)(che non conta perchè è l'identità) --- Esercizi:

1) Data la permutazione S8

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 5 & 7 & 1 & 3 & 6 & 8 \end{pmatrix}$$

Scrivere σ e σ^{-1} come prodotto di cicli disgiunti

Soluzione:
σ=(1 2 4 7 6 3 5)   7ciclo
σ^{-1}=(5 3 6 7 4 2 1)

2)
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 4 & 6 & 7 & 8 & 2 & 3 & 9 \end{pmatrix}$$

σ=(2 5 7)(3 4 6 8)   (sono identità (1) (9)
σ^{-1}=((2 5 7)(3 4 6 8)$)^{-1}$
=(3 4 6 8$)^{-1}$(2 5 7$)^{-1}$
=(8 6 4 3) (7 5 2) o stessa cosa (7 5 2)(8 6 4 3)

Perché questo?
Ricordiamoci che se f e g sono biettive f*g è biettiva
E il suo inverso ovvero $(f*g)^{-1}=g^{-1}*f^{-1}$

Regola:
Se σ= c1 c2 ….. Cr prodotto di cicli disgiunti
σ^{-1} =c^{-1}1 c^{-1}2…..c^{-1}r
Dove se Cv=(s1…Sk)
C^{-1}i=(Sk….S1)

---

3) Scrivere in forma matriciale i seguenti prodotti di cicli in S8
σ=(1 3 5 4)*(7 2 6)
Ɱ=(1 3 5 4)*(7 2 3)

Soluzione:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 5 & 1 & 4 & 7 & 2 & 8 \end{pmatrix} \mathcal{M} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 7 & 1 & 4 & 6 & 2 & 8 \end{pmatrix}$$

4) Scrivere la permutazione in S8

σ=(1 3 5)(2 5)(3 4 7 2)
Come prodotto di cicli disgiunti

Soluzione:
(1 3 4 7)(2 5)   identità:(6)(8)
Il tipo è (4,2)

Definiamo il tipo: il tipo di una permutazione σ è una K upla
(l1 l2…..lk) con l1>0l2>=.........>=lk t.c σ è prodotto di k cicli disgiunti ogniuno di lunghezza li

Es. se σ=(1 4 7 5 2)(3 8)(9 6)(11 12)
σ ha tipo (5,2,2,2)

---

5) Determinare il tipo di
σ=(1 2 3)(4 2 5)(1 7)
Trasformiamolo in prodotti di cicli

	σ=(1 7 2 3)(5 4) Il tipo di σ sarà (4,2) --- Quanti sono i 2 cicli in S5? Sono quanti i sotto insiemi si 2 elementi in un insieme di 5 elementi quindi: $\binom{5}{2} = \frac{5!}{2!(5-2)!} = \frac{5 \times 4 \times 3!}{2 \times 1 \times 3!} = \frac{5 \times 4}{2 \times 1} = \frac{20}{2} = 10$ La formula del coefficiente binomiale è: $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ --- Quanti sono i 3 cicli in S5? 1) Scelgo un sottoinsieme di 3 elementi in un insieme di 5 $\binom{5}{3}$ 2) Lo ordino in tutti i modi possibili 3! Possibilità 3) Identifico che abbia solo i cicli ottenuti ciclicamente ovvero dividendo per 3 Quindi il numero di 3 cicli in S5 è $\left(\binom{5}{3}\right) \cdot \frac{3!}{3} = 10 \cdot 2 = 20$ Regola il numero dei Kcicli in Sn(k<=n) è $\binom{m}{k} \cdot \frac{k!}{k} = \binom{m}{k} \cdot (k-1)!$
RIASSUNTO:	Scrivi qui il tuo riassunto:

Matematica discreta algebra geometría	Argomento trattato:
Lezione giovedì 26/10/2024	(matematica discreta) prof. Lea Terracini

Domande e risposte / parole chiave

$\uplus$ = unione disgiunta

Appunti:
Proprietà: ogni permutazione si scrive come prodotto di cicli disgiunti.
Teorema:
Se $\sigma \in S_n$ il numero di trasposizioni che intervengono in una composizione di σ (come prodotto di trasposizioni) è sempre pari o sempre dispari.
Dimostrazione:
Supponiamo per assurdo
$\sigma=S_1\ldots\ldots S_k=t_1\ldots\ldots t_h$ dove S_i,t_i trasposizioni k pari, h dispari
Moltiplicando entrambi i membri per $S_k\, S_{k-1}\ldots\ldots S_1$
trovo:$(1)=S_k\, S_{k-1}\ldots\ldots S_1T_1\ldots\ldots T_k$
Quindi L'identità si scrive come prodotto di un numero dispari di trasposizioni
$(1)=S_1\, S_2\ldots\ldots S_l$ (L dispari)
$S_i=(a_i\, b_i)$ $a_i\neq B_i$
Supponiamo che 1 compaia nella decomposizione.
Nota bene non può comparire solo una volta!
$(1)=(1\ x)\quad (a\ b)\quad (1\ y)$
"Avviciniamo" tra loro le due occorrenze di 1 con le regole seguenti:

1) Se $(1\ x)$ e $(a\ b)$ sono disgiunti
   Allora: $(1\ x)\,(a\ b)=(a\ b)\,(1\ x)$ (perchè commutano)
   Ho avvicinato $(1\ x)$ e $(1\ y)$ di un posto
2) Se $(1\ x)$ e $(a\ b)$ non sono disgiunti
   Allora: $(a\ b)=(a\ x)$ (un termine sarà uguale)
   $(1\ x)\,(a\ x)= (a\ x)\,(1\ a)$
   Sostituisco e diventa $(a\ x)\,(1\ a)\ldots\ldots(1\ y)$
   Iterando si ottiene una situazione del tipo:
   $(1) =\ldots\ldots(1\ x)\,(1\ y)\ldots\ldots$
   Arrivati qui abbiamo 2 situazioni
   a) Se $x=Y$ posso cancellare le occorrenze
   b) Se $x\neq y$ uso la regola
      $(1\ x)(1\ y)=(1\ y)(x\ y)$
      $(1)=\ldots\ldots(1\ y)(x\ y)\ldots\ldots$(cancello uno dei due)

Le occorrenze di 1 scendono di 1 , Si arriva a una situazione in cui spariscono le occorrenze di 1
Ripetendo con altri numeri si arriva ad un assurdo.

Permutazioni pari si scrivono come prodotto di un numero pari di trasposizioni.

Permutazioni dispari si scrivono come prodotto di un numero dispari di trasposizioni

P_n=permutazioni pari in S_n
D_n= permutazioni dispari in S_n

$S_n=P_n \uplus D_n$

Proviamo ora che se $N>=2$
$|P_n|=|D_n|=n!/2$

Dimostro che esiste una biezione Pn→Dn
F: Pn→Dn
Pari σ→σ(1 2) (dispari)
Proviamo che F è iniettiva se F(σ)=F(**τ**)
Allora σ(1 2)=**τ**(1 2) allora σ=**τ**
Suriettiva sia **v** є Dn
Pongo σ = **v** (1 2) (1 2) = **v**
Quindi |Pn|=|Dn|=n!/2

Esempio:

(1 3 5 4 2 6)=(1 6)(1 2)(1 4)(1 5)(1 3) (è dispari)
(1 3 5)(4 2 6)=(1 5) (1 3) (4 6) (4 2) (è pari)

In generale in un L ciclo
(S1…..Sl)=(S1 Sl) (S1 Sl-1)....(S1 S2)
Quindi un L ciclo è paro se L dispari
Dispari quando L è pari
Nota bene L'identità è una permutazione pari !

Supponiamo σ, **τ** Є Sn

σ	**τ**	σ***τ**
Pari	pari	pari
dispari	dispari	pari
pari	dispari	dispari
dispari	pari	dispari

Se σ Є Sn il tipo di σ è (l1….lk)
Con l1>=l2>=.....lk t.c. σ si decompone in k cicli disgiunti ognuno di lunghezze Li
Es.

Se σ ha tio(5 5 4 3 3 3)σ è dispari

In generale se σ ha tipo (Li….Lk)

σ è pari ⇔ $\sum_{i=1}^{K}$ (L1-1) è pari

σ è pari ⇔ $\sum_{i=1}^{K}$ (Li-1) è dispari

$\sum_{i=1}^{K}$ (li-1) modulo 2

Periodo di una permutazione
Es. σ=(1 5 7 3 2 9) calcolo $σ^2$ $σ^3$ $σ^4$……
$σ^2$=(1 7 2)(5 3 9)
$σ^3$=(1 3)(5 2)(7 9)
$σ^4$=(1 2 7)(3 5 9)
$σ^5$=(1 9 2 3 7 5)= (9 2 3 7 5 1)
$σ^6$=(1)(identità) quindi $σ^6$=$σ^{12}$=$σ^{18}$=.......$σ^{6k}$(1)

	Deduciamo che per (σ)=6 ovvero 6 ha periodo 6 Definizione: sia σ Є Sn il minimo intero n>0 t.c. σ^n=(1) si dice periodo di σ e si denota per (σ) Esempi: periodo ((1 2))=2 Periodo ((1 2 3))=3 In generale se σ=(s1…..sl)è un L ciclo allora per (σ)=l Supponiamo σ=(1 2)(3 4) σ^2=(1 2)(3 4)(1 2)(3 4) =$(1\ 2)^2(3\ 4)^2$=(1) periodo di σ^2=2 supponiamo σ=(1 2 3) (4 5) $\sigma^2=(1\ 3\ 2)^2(4\ 5)^2$(4 5 sono l'identità quindi scompaiono)=$(1\ 3\ 2)^2$=(1 2 3) $\sigma^3=(1\ 3\ 2)^3$(si elimina perchè è l'identità)$(4\ 5)^3$ ….. σ^6=(1) periodo σ =6 proprietà : se σ e **τ** sono cicli disgiunti di periodi n e m rispettivamente per (σ***τ**)=mcm (n,m) Proposizione se σ ha tipo (l1….lk) Allora per (σ)=mcm(l1….lk) Sapere il periodo è utile per fare conti sulle permutazioni Oss. sia σ=(1 2 3 4 5 6) Vogliamo calcolare σ^{1052} Sappiamo 1052:σ=175 resto 2 1052=6*175+2 Quindi $\sigma^{1052}=\sigma^{6*175+2}=\sigma^{6*175}*\sigma^2=\sigma^2$ =(1 3 5) (2 4 6) (la prima parte si elimina perchè è un multiplo dell'identità)
RIASSUNTO:	Scrivi qui il tuo riassunto:

Matematica discreta algebra geometría	Argomento trattato:
Lezione giovedì 05/11/2024	Aritmetica (matematica discreta) prof. Lea Terracini
Domande e risposte / parole chiave	Appunti: L'aritmetica è lo studio dei numeri interi Z={......-3,-2,-1,0,1,2,3…..} Possiamo fare 2 operazioni primitive: 1) Addizione "+"→risultato somma 2) Moltiplicazione "*"→risultato prodotto Proprietà delle operazioni: -Entrambe sono associative e commutative $\forall$ a,b,c $\in$ Z a+(b+c)=(a+b)+c a*(b*c)=(a*b)*c a+b=b+a a*b=b*a -hanno entrambe un elemento neutro 0 per l'addizione 1 per la moltiplicazione -ogni elemento in Z ha un inverso che chiameremo opposto rispetto all'addizione a+(-a)=0 $\forall$a$\in$Z -questo non è vero per la moltiplicazione solo +1 e -1 sono invertibili rispetto alla moltiplicazione $1^{-1}=1$ $(-1)^{-1}=-1$ -proprietà distributiva del prodotto rispetto alla somma: $\forall$a,b,c $\in$ Z a(b+c)=ab+ac Possiamo dire che Z è un anello perchè 2 operazioni soddisfano le stesse proprietà Ogni elemento di Z è un numero naturale tipo: 0 , 1 , 1+1 , 1+1+1… O l'opposto di un numero naturale: -1 -2

N={numeri naturali}
Sottrazione a-b=a+(-b)
Ordine su Z a=b se b-a ∈ N

Struttura moltiplicativa di z

Nozione di divisibilità:

Definizione: siano a,b,∈ Z diciamo che a divide b(a è un divisore di b)o (b è un multiplo di a)

E scriviamo a|b

Se esiste C ∈ Z t.c b=a*c
Esempi:
2|6 6=2*3   -2|6   6=(-2)*(-3)
2|-6 -6=2*-3   -2|-6 -6=(-2)*(3)

-n|n si può sempre fare perchè n=n*1
N|-n (divide il suo opposto) -n=n*(-1)

-ogni elemento divide 0
0=n*0 ∀n
-0 è multiplo di se stesso
-+ e - 1 dividono ogni n ∈ Z
-inoltre se m|n ∀m ∈ Z allora m=+-1
-supponiamo:
N|a e n|b → n|a+b   n|a-b

a=n*a1   b=n*b1

Allora a+b=n*a1+n*b1=n(a1+b1)
Allora n|a+b

-inoltre se n|a allora n|a*b per ogni b n è multiplo di a

-è sempre vero che n|ab allora n|a o n|b ?
No!
Es. n=6 a=2 b=3
n|ab   n∤a e n∤b

Definizione: sia n≠,1,-1 diciamo che 0 è irriducibile se gli unici divisori di n sono +-1 e +-n cioè se:
n=a*b allora uno tra a e b è +-1
Diciamo che n è riducibile se non irriducibile
Diciamo che n è primo se
∀a,b ∈ Z n|ab allora n|a0 n|b

Es +-6 non è primo
+-7 è primo
proprietà : se n è primo allora n è irriducibile

Se vuoi vedi dimostrazione sul quaderno

Teorema: se $\forall$ a,b,c $\in$ Z $b\neq 0$ (a dividendo e b divisore)
Esistono e sono unici due interi q(quoziente) r (resto
T.c. $a=bq+m$ e $0<=m<|b|$

Osservazione: basta dimostralo nel caso in cui:
$a>=0$ $b>0$
Infatti consideriamo per esempio
$a=2575$ $b=14$

$2575=183*14+13$

Dimostrazione nel caso $a>=0$ $b>0$
Trovo il risultato per induzione su a
Esistenza: $a=0$
$0=0*b+0$ $q=0$ $r=0$
Suppongo il risultato vero $\forall a1>a$ e lo dimostro per a

Se $0<=a<b$ $a=0*b+a$ $q=0$ $r=a$
Se $a>=b$ pongo $a1=a-b<a$
Posso applicare ad a1 l’ipotesi induttiva
$a1=b*q1+r$ con $0<=r<b$
$a-b=bq1+r$
$a=bq1+b+r$
$=b(q+1)+r$
Dimostro l’unicità:
Supponiamo che
$a=bq+r=bq1+r1$ con $q,q1,r,r1 \in Z$
E $0<=r,r1<b$
Allora $0<r1-r<b$
$r1-r=bq-bq1=b(q-q1)$
Quindi r1-r è un multiplo di b non negativo$<b$
$r1-r=0$ allora $m1=m$
$q-q1=0$ allora $q1=q$
Allora l’unicità è dimostrata

RIASSUNTO:	Scrivi qui il tuo riassunto:

Matematica discreta algebra geometría	Argomento trattato:
Lezione giovedì 12/11/2024	Algoritmo di euclide e identità di bézout (matematica discreta) prof. Lea Terracini
Domande e risposte / parole chiave	Appunti: Notazione posizionale: È un sistema di scrittura dei numeri naturali mediante cifre il cui valore dipende dalla posizione in cui si trovano Esempio: $67942 = 6 \cdot 10^4 + 7 \cdot 10^3 + 9 \cdot 10^2 + 4 \cdot 10^1 + 2 \cdot 10^0$ 67942=10*6794+2 6794=10*679+4 679=10*67+9 67=10*6+7 6=10*0+6 -ogni quoziente diventa dividendo al passo successivo -i resti in ordine danno la scrittura del numero --- Definizione: sia b>=2 un numero intero (base) e sua c un insieme di simboli (cifre) che rappresentano i numeri in {0,1….b-1} si dice notazione posizionale di un numero m∈N in una base b una successione di cifre m=ck ,ck-1……c0 con c0,c1……ck∈C m=ck*b^k+ck-1*b^{k-1}+....+c1b+c0 Esempi: La base binaria b=2 c={0,1} 0→0 1→1 10=1*2+0=2 11= 1*2+1=3 100=1*2^2+0.2+0*1=4 101=1*2^2+0*2+1*1=5

b=3 c={0,1,2}

0 1 2
10=3
11=4
12=5
20=6

22=2*3+2*1=8

$2102=2*3^3+1*3^2+0*3+2*1=54+9+2=65$

Convertiamo adesso 587 in base 3
587=3*195+2
195=3*65+0
65=3*21+2
21=3*7+0
7=3*2+1
2=3*0+2

587=210202

Osservazione: se b<=10 c={0,1,.....,b-1}
Se b>10 c={0,1,......,9,A,B,C…}

Esempio se b=13
2 BA7=$2*13^3+11*13^2+10*13+7$

Algoritmo di euclide per il mcd

Esempio: vogliamo calcolare mcd(3575,654)

3575=654*5+305
654=305*2+44
305=44*6+41
44=41*1+3
41=3*13+2
3=2*1+1
2=1*2+0

L'ultimo resto non nullo è il mcd

mcd(1475,105)
14575=105*138+85
105=85*1+20
85=20*4+5
20=5*4+0

Regola generale per calcolare mcd (a,b)
Posso supporre a,b≠0

B≠0
a=bq1+r1   b>r1>=0

	b=r1q2+r2 b>r1>r2>=0
	r1=r2q3+r3 b>r1>r2>r3>=0
	
	rn-3=rn-2 qn+rn-1
	rn-2=rn-1qn+rn rn è mcd
	rn-1=rnqn+1+0
	
	d=rm provo che d|a e d|b
	
	Infatti rn|rn-1 (ultima riga)
	d|rn d|rn-1 →d|rn-2 (penultima riga)
	d|rn-1 d|rn-2 → d|rn-3 (terzultima riga)
	Ecc….
	Risalendo troviamo d|b d|a
	Proviamo che d è il massimo divisore comune di a,b
	Sia c un divisore di a e b provo che c|d
	Percorrendo la successione di uguaglianza dall'alto al basso si trova:
	
	c|a c|b c|r1 c|r2…… c|rn=d
	Allora d è il massimo comune divisore
	
	Identità di bézout
	
	Siano a,b appartenenti a Z non entrambi nulli (b≠0)
	E sia d=(a,b)
	Allora esistono (non unici) A,B appartenenti a Z t.c. d=Aa+Bb
	Percorrendo a ritroso le uguaglianze dell'algoritmo di euclide, troviamo
	d=rn=rn-2-qn rn-1(penultima uguaglianza)
	      =rn-2-qn(rn-3-qn-1)rn-2
	
	Possiamo usare la riga precedente per scrivere rn-2 come combinazione lineare di rn-3,rn-4 ecc….
	
	Risalendo si scrive d=Aa→Bb
	
	Calcolare Mcd(126,35) e scrivere l'identità di bétout
	
	126=35*3+21
	35=21*1+14
	21=14*1+7 nosto mcd
	14=7*2+0
	
	Bézout
	7=21-14
	=21-(35-21)
	=-35+2*21
	=-35+2*(126-3*35)
	=2*126+(-7)*35 (A=2 B=-7)
	
	Osservazione: ci sono infiniti A,B t.c d=Aa+Bb
	
	Infatti se so che d=A0a+B0b e M è un multiplo comune di A e B
	Posso scrivere:
	d=A0a+B0b
	  =A0a+b0b+m-m

	=A0a+B0b+m1a-m2b =(A0+m1)a+(B0-m2)b (sarà A) (questa sarà B) Nel nostro esempio 7=2*126+(-7)*35 =(2+5k)*126+(-7-18k)*35 =5*126=18*35
RIASSUNTO:	Scrivi qui il tuo riassunto:

Matematica discreta algebra geometría	Argomento trattato:

Lezione giovedì 12/11/2024	Aritmetica modulare (matematica discreta) prof. Lea Terracini

Domande e risposte / parole chiave

Ξ = relazione di congruenza

Appunti:
L'aritmetica modulare serve per contare in modo ciclico es: ore settimane …
Nei cicli per esempio calcoliamo il periodo $\sigma \in S_n$
per (σ) =mcm $\{k>0|\sigma^k=(1)\}$
$\sigma=(1\ 2\ 3)$ per $(\sigma)=3$
σ =id $\sigma^1=\sigma$ $\sigma^2=(1\ 3\ 2)$ σ^3 = id

Per esempio se per σ =5 $\sigma^{131242}=\sigma^2$
Le potenze di σ si calcolano modulo il periodo della permutazione nel nostro caso σ

Dato $n \in N$, $n >=2$ modulo
Definiamo una relazione su Z ponendo
$\forall$ a, b $\in$ Z
Relazione di congruenza aΞb mod N (o anche $a\Xi_n b$)

("a è congruo a b modulo n)
Se n|a-b
Esempi:

8Ξ1 mod 7 infatti 7/ 8-1 =7
1Ξ-1 mod 2 infatti 2/ 1-(-1)=2
5Ξ-7 mod 12 infatti 12 / 5-(-7)=12
5Ξ-7 mod 6 infatti 6/ 12
5Ξ7 mod 6 perchè $6\nmid 5-7=-2$

Proposizione: la relazione di congruenza modulo n è una relazione di equivalenza.

Dimostrazione:
-verifichiamo che sia riflessiva : $\forall$ a $\in$ Z aΞa mod n infatti n/a-a=0
-proprietà simmetrica: supponiamo aΞb mod n quindi n/a-b quindi n/b-a=-(a-b) e quindi bΞa mod n
-transitiva: supponiamo aΞb mod n, bΞc mod n quindi n/a-b n/b-c ma allora (a-b)9(b-c)=a-c
⇒aΞc mod n

Definiamo per a $\in$ Z , la classe di equivalenza $[a]_n$ (o anche $\bar{a}$)
$[a]_n$){b $\in$ Z | aΞb mod n} classe di resto di a modulo n

Osservazione aΞb mod n significa che b=a+kn per qualche k$\in$ Z
Quindi $[a]_n$){a+kn|k$\in$ Z}

Esempi in n=5

$[0]_5$=5z{.....-20,-15,-10,-5,0,5,10,15……}
Sarà uguale a $[5]_5=[-20]_5$
$[1]_5$=1+5Z={...14,-9,-4,1,6,11,16….}
$[2]_5$=2+5Z={......13,-8,-3,2,7,12,17…}
$[3]_5$=3+5Z={......-2,3,8,13,18….}
$[4]_5$=4+5z={....-16,-11,-6,-11419,14,19…}

Ci sono esattamente 5 classi di resto mod 5

Proposizione
Sia $a \in \mathbb{Z}$ allora:

$$[a]_n=[r]_n$$

Dove m è il resto della divisione a per n (quindi $0<=m<n$)

dimostrazione :
Per l'algoritmo di divisione $a=nq+r$
Quindi $a-r=nq \Rightarrow a \equiv m \mod n \Rightarrow [a]_n=[r]_n$
D'altra parte se $0<=r<s<=n-1$ non è possibile che $n/s-r$ quindi $r \not\equiv s \mod n$ e quindi $[r]_n \neq [s]_n$
⟿le classi modulo n sono
$[0]_n$, $[1]_n$,$[2]_n$,.....,$[n-1]_n$
E queste sono tutte distinte.
Se $r \in [a]_n$ e $0<=r<=n-1$
r si dice rappresentate canonico della classe

Es. 2 è rappresentante canonico di $[17]_5$
$[2]_5=[17]_5=[2002]_5$
Sia Zn={classi di resto modulo n}
$=\{[0]_n,[1]_n, \ldots,[n-1]_n \}$
$|Zn|=n$

Osservazione: c'è una funzione naturale (suriettiva non iniettiva)
$\pi n: Z \to ZN$
$a \mapsto \bar{a}$

Operazioni su Zn con n fissato $\bar{a}=a[n]_n$
-addizione:

Dati $\bar{a},\bar{b} \in Zn$ definisco (classi di resto) $\bar{a}+\bar{b} =a+b$ (rappresentanti)

Devo verificare che la definizione non dipende dalla scelta dei

rappresentanti cioè che se $\bar{a}^1=\bar{a}$ e $\bar{b}^1=\bar{b}$ allora $\overline{a^1+b^1}=\overline{a+b}$

La verifica guardala sul quaderno.

Esempi
$[2]_2 + [9]_2 =[2+9]=[11]_2 =[1]_2$ (rappresentante candidato)
= =
$[0]_2+[5]_2$ $[0+5]_2=[5]_2[1]_2$

$[-5]_7+[6]_7 =[1]_7$
=
$[2]_7+[6]_7=[8]_7=[1]_7$

Moltiplicazione in Zn

Dati $\bar{a},\bar{b} \in Zn$ definisco $\bar{a}*\bar{b} =\bar{a}*\bar{b}=ab$
Di nuovo devo provare che la definizione non dipende dalla scelta dei rappresentanti , cioè:
Se $a^1 \equiv a \mod n$ e $b^1 \equiv b \mod n$
Allora devo provare che $a^1b^1 \equiv ab \mod n$
$a^1=a+kn$

$b^1=b+hn$
$a^1b^1=(a+kn)(b+hn)=ab+n(ah+bh+kh)$
⇒anche la moltiplicazione è ben definita

Esempi:
$[3]_5[7]_5=[3.7]_5=[21]_5=[1]_5$
-risolvere modulo 7

$$\left((\overline{3}\cdot\overline{5})\cdot(\overline{2}-\overline{6})\right)\cdot\overline{3}$$

$$(\overline{1}\cdot\overline{3})\cdot\overline{3}$$ =3*3=9=2 (tutto col trattino sopra ovviamente)

Proprietà delle operazioni su Zn

a) L'addizione è associativa, commutativa $\bar{0}$ è l'elemento neutro , e ogni elemento ha un opposto:

   $-\bar{a}=\overline{-a}$
   esempio : $-[3]_7=[-3]_7=[4]_7$

b) La moltiplicazione è associativa , commutativa $\bar{1}$ è elemento neutro
   Non è vero che ogni elemento ha inverso moltiplicativo: per esempio $\bar{0}$ non è invertibile
   Ma per esempio: $[2]_5*[3]_5=[6]_5=[1]_5$
   Quindi è invertibile

c) Vale la proprietà distributiva del prodotto rispetto alla somma:

   $$[a]\cdot\left([b]+[c]\right)=\left([a]\cdot[b]\right)+\left([a]\cdot[c]\right)$$

RIASSUNTO:	Scrivi qui il tuo riassunto:

Matematica discreta algebra geometría	Argomento trattato:
Lezione giovedì 22/11/2024	Operazioni in Zn ((matematica discreta) prof. Lea Terracini
Domande e risposte / parole chiave 三 = relazione di congruenza	Appunti: Operazioni su Zn: -addizione [a]+[b]=[a+b] -moltiplicazione [a]*[b]=[a*b] Ben definite Proprietà delle operazioni in Zn Addizione: associatività,commutatività, $\bar{o}$ elemento neutro ogni elemento ha un opposto: $-\bar{a}=\overline{-a}$ -moltiplicazione: associativa, commutativa, $\bar{1}$ elemento neutro -proprietà distributiva di * rispetto a + ((Zn,+,*) è un anello) Invertibilità moltiplicativa in Zn: non è vero che ogni elemento in Zn ha un inverso moltiplicativo: $\bar{o}$ non è mai invertibile , perché $\bar{o}*\bar{a}=\bar{o}\neq 1$ Consideriamo invece $\bar{2}$ in Z_6 $\bar{2}*\bar{o}=\bar{o}$ $\bar{2}*\bar{1}=\bar{2}$ $\bar{2}*\bar{2}=\bar{4}$ $\bar{2}*\bar{3}=\bar{o}$ $\bar{2}*\bar{4}=\bar{2}$ $\bar{2}*\bar{5}=\bar{4}$

$\rightsquigarrow \overline{2}\neq\overline{1} \quad \forall \overline{x} \in Z_6 \rightsquigarrow \overline{2}$ non è invertibile

Invece $\overline{2}$ in z_3 : $\overline{2}*\overline{2}=\overline{1} \rightsquigarrow \overline{2}^{-1}=\overline{2}$

In z_5 , $\overline{2} * \overline{3}=\overline{1}$ quindi $\overline{2}^{-1}=\overline{3}$

Caratterizzazione degli elementi invertibili in Zn

-n=2

	ō	$\overline{1}$
ō	ō	ō
$\overline{1}$	ō	$\overline{1}$

1 invertibile

-n=3

$Z_3^{\star}=\{\overline{1}\ ,\ \overline{3}\ \}$

	ō	$\overline{1}$	$\overline{2}$
ō	ō	ō	ō
$\overline{1}$	ō	$\overline{1}$	$\overline{2}$
$\overline{2}$	ō	$\overline{2}$	$\overline{1}$

O nn invertibile 1,2 invertibili

-n=4

$Z_4^{\star}=\{\overline{1}\ ,\ \overline{3}\ \}$

	ō	$\overline{1}$	$\overline{2}$	$\overline{3}$
ō	ō	ō	ō	ō

$\overline{1}$	ō	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	ō	$\overline{2}$	$\overline{1}$	$\overline{2}$
$\overline{3}$	ō	$\overline{3}$	$\overline{2}$	$\overline{1}$

0 e 2 non invertibili
1 e 3 invertibili
Poniamo
$Z_n^{☆}$ = {ā є Zn | ā invertibile}

n=5

	ō	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
ō	ō	ō	ō	ō	ō
$\overline{1}$	ō	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	ō	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	ō	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	ō	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

n=6

	ō	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
ō	ō	ō	ō	ō	ō	ō
$\overline{1}$	ō	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{6}$
$\overline{2}$	ō	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	ō	$\overline{3}$	ō	$\overline{3}$	ō	$\overline{3}$
$\overline{4}$	ō	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	ō	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Poniamo $\varphi(n)=|Z^{☆}n|$, $\varphi(1)=1$
$\varphi(1)=1$
$\varphi(2)=2$
$\varphi(3)=2$
$\varphi(4)=2$
$\varphi(5)=4$
$\varphi(6)=2$
$\varphi(7)=6$
$\varphi(8)=4$

Caratterizzazione degli elementi invertibili in Zn

	Sia $\bar{a} \in Zn$ $\bar{a}$ è invertibile in Zn $\Leftrightarrow$ $\exists \bar{b} \in Zn$ t.c. $\overline{ab} = \bar{1}$ ((a,n)=1) Teorema: 1) $\bar{a} \in Zn^{*} \Leftrightarrow$ (a,n)=1 (ovvero se un rappresentante di a è coprimo con n) 2) Inoltre se (a,n)=1 e Aa+Bb=1 è l'identità di bezout allora $\bar{a}^{-1}=\bar{A}$ supponiamo (a,n)=1 Bèzout: $\exists$ A,B Aa+Bn=1 $\bar{A}\bar{a}+\overline{B}\bar{n} = \bar{1}$ in zn $\Rightarrow \bar{A}\bar{a}=1$ in Zn $\rightarrow \bar{a}^{-1}=\bar{A}$ $\bar{a}^{-1}$ è la classe in Zn del coefficiente di $\bar{a}$ nell'identità di bèzout Esempio Z42 dire se le seguenti classi di resto sono invertibili in caso affermativo determinare l'inverso 5,14 13 Soluzione: Si ha (5,42)=(13,42)=1 5,13 appartengono $Z^{*}42$ (14,42)≠1 Cerchiamo $\bar{5}^{-1}$ →applico euclide a 42,5 42=5*8+2 5=2*2+1 2=2*1=0 bèzout 1=5-2*2 =5-2(42-5*8) =17*5-2*42 → $\bar{5}^{-1} = \overline{17}$ Prova: 5*17=85=42*2+1 $\equiv$1 mod 42 Calcoliamo $\overline{13}^{-1}$ applico euclide alla copia 42,13 42=13*3+3 13=3*3+1 3=3*1+0 Bèzout: 1=13-4*3 =13-4(42-3*13)=13*13-4*42 Allora $\overline{13}^{-1} = \overline{13}$ in Z_{42} Prova: 13*13=163=42*4+1$\equiv$1 mod 42 In Z_{55} dire se le seguenti classi di resto sono invertibili in caso affermativo determinare l'inverso : 2,3,5,33,39 <hr>(fatto sul quaderno) $Zn^{*}=\{\bar{a} \in Zn \mid \bar{a}$ invertibile$\}$ $=\bar{a} \in Zn \mid (a,n)=1\}$

In particolare se n=p è primo
$(a,p)=1 \Leftrightarrow p \nmid a$
$Zp^{☆}=\{\bar{a} \in Zp \mid p \nmid a\}$
Poichè p/0 e $p \nmid j$ $\forall j=1\ldots\ldots,p-1$

$Zp^{☆}=\{\bar{1},\bar{2},\bar{3},\ldots,\overline{p-1}\}=Zp-\{\bar{o}\}$
$\varphi(p)=p-1$
Se p è primo $\Leftrightarrow$ p è un campo
$\varphi(p^2)=?$
$Zp^2=\{0,1\ldots.p,p+1,\ldots.,2p,\ldots,3p,\ldots.,(p-1*p,p^2-1\}$
$Zp^{2☆}=\{\bar{a} \in Zp \mid p \nmid a\}$
$\varphi(p^2)=p^2-p$
$\varphi(p^3)=p^3-p^2$
$\varphi(p^n)=p^n-p^{n-1}=p^{n-1}(p-1)$

Zero-divisori in Zn
In Z $ab=0 \Rightarrow a=0$ oppure $b=0$
In Zn questo in generale non è vero
2*3=0 in z6
Definizione: $\bar{a}\neq\bar{0}$ è uni zero-divisore in zen se $\exists \bar{b} \in Zn$, $\bar{b}\neq\bar{0}$ t.c. $\overline{ab}=\bar{0}$
Es 2,3 sino 0-divisori in z6
2 è 0 divisore in z4: 2*2=0

osservazione : se $\bar{a} \in Zn^{☆}$ $\bar{a}$ non è zero-divisore ab=0 moltiplico per a^{-1}
$a^{-1}\,ab=0 \Rightarrow b=0$
(i campi non contengono 0 divisori)
Proposizione
$\bar{a} \in Zn$ con $\bar{a}\neq 0$ è uno zero-divisore se $(a,n)\neq 1$ cioè:
$\Leftrightarrow \bar{a}$ non è invertibile
Questo prova che n non primo allora n non è un campo infatti a/n $\bar{a}$ è uno zero divisore in Zn
$\Rightarrow$Zn non è un campo

RIASSUNTO:	Scrivi qui il tuo riassunto:

Matematica discreta algebra geometría	Argomento trattato:
Lezione giovedì 26/11/2024	Strutture algebriche. Semigruppi, monoidi e gruppi. Esempi. Prime proprietà dei gruppi.((matematica discreta) prof. Lea Terracini
Domande e risposte / parole chiave 三 = relazione di congruenza	Appunti: Gruppi: Struttura algebrica: insieme sun cui è definito un certo numero di operazioni; (x,☆1,☆2…..,☆n)☆i operazione su x x X x→x (x1,x2)→x1☆x2 Esempi: (sn,0) o permutazioni di composizioni (Z,+,*)(Q,+,*)(R,+,*)(C,+,*)(K,+,*) Guarderemo insiemi con solo 1 operazione (x,☆) Def: una struttura algebrica (x,☆) si dice: -semigruppo se ☆ è associativa -monoide se ☆ è associativa ed esiste un elemento neutro -gruppo se: a) ☆ è associativa b) esiste elemento neutro c)ogni elemento ammette inverso

Se ☆ è commutativa, parliamo di semi gruppo , gruppo, commutativo o gruppo abeliano
Osservazione:
☆ deve essere ben definita su x, cioè
∀x,yЄ x   x☆yЄx
Esempi:

1)(N,+) monoide commutativo 0 è il suo elemento neutro
Solo 0 ha inverso (opposto) rispetto “+”

2)(N,-) non è struttura algebrica perchè la sottrazione non è ben definita su n

3)(N-{0},+) è una struttura algebrica ☆ è associativa non c’è elemento neutro (è un semigruppo commutativo)

Def: sia(x,☆) una struttura algebrica Y⊆X si dice chiuso o stabile rispetto a ☆ se ∀a,bЄY si ha a☆BЄY

4)(Z,+) è un gruppo commutativo

5)(Z-{0},+) non è una struttura algebrica perchè Z-{0} non è stabile rispetto alla somma 1,-1ЄZ-{0} ma 1+(-1)=0

6)(Q,+),(R,+),(C,+),(K,+) sono gruppi abeliani

7)(Z,*) è un monoide commutativo con 1 come elemento neutro solo +-1 sono invertibili

8)(Zn,+) gruppo abeliano
9)(Q,*),(R,*),(C,*),(K,*) monoide commutativo nota bene non è un gruppo perchè 0 non è invertibile

10) poniamo Q☆=Q-{0},R☆=R-{0},C☆=C-{0},K☆=K-{0}
(Q☆,*)
Osserviamo che il prodotto è un operazione su K☆, infatti xy=0 allora x=0 oppure y=0 quindi k☆ è chiuso rispetto al prodotto
E ogni elemento non nullo è invertibile

11)Zn☆={āє Zn |ā invertibile rispetto al prodotto}
={āє Zn |(a,n)=1}
(Zn☆ è una struttura algebrica perchè:
-1,1 є Zn☆ ma 1+-1=0є Zn☆
(Zn☆,*) è una struttura algebrica
Infatti Zn☆ è chiuso rispetto al prodotto:
Se a, b є Zn☆ si ha ab=ab
se(a,n)=1 e (b,n) allora (ab,n)=1
(Zn☆,*) gruppo commutativo

12) Y insieme non vuoto
x=p(y)=insieme delle parti di Y ={A|A⊆Y}
(x,∪) (x,∩) strutture algebriche
Sia l’unione sia l’intersezione sono associative e commutative
Ø è l’elemento neutro per l’unione
Infatti A∪Ø=A

y è elemento neutro per l'intersezione
Infatti A∩y=A ∀AϵX
L'unico elemento invertibile rispetto a ∪ è Ø
Per ∩ Ø non è invertibile l'unico elemento invertibile è y
(x,∪) (x,∩) sono monoidi commutativi (non gruppi)

13) monoide delle parole monoide libero A insieme non vuoto (alfabeto)
p={stringe finite di elementi di a}
={[](stringa vuota),[a],[b],[c]....[a a]...[ab]...}
Definiamo su p l'operazione di giustapposizione ☆
[a1…ak]☆[b1…bh]=[a1…..akb1…bh]
(p,☆) ☆ associativa non commutativa se |A|>1
[]elemento neutro
Solo [] è invertibile
P è un monoide non commutativo

14) X iniseme |x|>=2
F(x),0)
La composizione (o)
La composizione (o) è associativa
Idx :x→x elemento neutro (identità)
X→x
Non ogni funzione ha inversa esistono infatti funzioni non iniettive in F(x) (per esempio quelle costanti)
o non è commutativa: per esempio se x{a,b}
f(a)=f(b)=a
g(a)=b,g(b)=a
g(a)=b , g(b)=a
f o g: a→a g o f: a→b
b→a b→b
⇒ (F(x) , o) monoide non commutativo

15) poniamo S(x) ={FϵS(x)|F biettiva}
È chiuso rispetto alla composizione
(S(x),0) è un gruppo detto gruppo delle permutazioni su x (gruppo simmetrico su x)
Caso particolare x{1…n}=In
S(x) Sn gruppo simmetrico su n elementi non commutativo se n>=3

16) m(n,k)={matrici quadrate n x n a coefficente su k}
Gln(k){⋉ ϵ M(n,k)|det ⋉ ≠0}
gln= gruppo lineare di ordine n a coefficiente in k (non commutativi se n>2)

Osservazione:
Dato un gruppo (G,☆) si usa di solito la notazione moltiplicativa
a☆b=ab
a^n0a☆a☆a….☆a
a^{-1}=inverso di a

Per certi gruppi abeliani si usa la notazione additiva (Z,+),(Q,+),(k,+)
a☆b=a+b
na=a+a+...+a
-a= inverso di a (opposto)

	Proposizione: sia (G, ☆) un gruppo: a) L'elemento neutro è unico b) $\forall$ x є G l'inverso di x è unico c) $\forall$ x,y є G $(x☆y)^{-1}=y^{-1} ☆ x^{-1}$ d) Valgono le leggi di cancellazione destra e sinistra , cioè: $\forall$ x,y,z є G $x☆y=x☆z \Rightarrow y=z$ $z☆y=z☆y \Rightarrow x=z$
RIASSUNTO:	Scrivi qui il tuo riassunto:

Matematica discreta algebra geometría	Argomento trattato:
Lezione giovedì 28/11/2024	I gruppi ((matematica discreta) prof. Lea Terracini

Domande e risposte / parole chiave

☰ = relazione di congruenza

Appunti:
Gruppi
(G, ☆) ☆:G→G
a)☆ associativa
b)esiste elemento neutro
c) ogni elemento ha inverso

Esempi: Z,Q,R,C,K,Zn →+
Q☆,R☆,C☆,K☆,Zn☆ k☆=k-{0}→*
Scriveremo semplicemente
Z,Q,R,C,K,Zn
Q☆,R☆,C☆,K☆,Zn☆
Sottintendendo l'operazione di gruppo

Gruppi non commutativi
(Sn,(0)) (gln(k),*)
gln(k)={⋉ є M(n,k)-det ⋉ ≠0}

Prodotto diretto di gruppi
Siano (G1,☆1) e (G2,☆2) gruppi
Considero il prodotto cartesiano
G1xG2={(a,b)-a є G1, b є G2}
Definiamo su G1xG2 l'operazione ☆
Ponendo ∀(a1,b1),(a2,b2) є G1 x G2
(a1,b1)☆(a2,b2)=(a1☆1 a2, b1☆2 b2)

(G1 x G2,☆) è un gruppo
Infatti
a)☆ è associativa
b)esiste elemento neutro
c)ogni (a,b) є G1xG2 ha inverso

(G1 x G2,☆) è un gruppo detto diretto di G1 e G2
G1 x G2
Esempi:

- Z2 x Z3 (Z2,+) (Z3,+)
  Z2={[0],[1]}
  Z3={[[0]],[[1]],[[2]]}
  Z2 x Z3={[0] [[0]]),([0],[[1]]),([0] [[2]]),([1] [[0]]),([1] [[1]]),([1] [[2]])

Tavola dell'operazione sul prodotto diretto

	([0][0])	([0][[1]])	([0] [[2]])	([1] [[0]])	([1] [[1]])	([1] [[2]])
([0][0])	([0][0])	([0][[1]])				
([0][[1]])	([0][[1]])					
([0] [[2]])	([0] [[2]]			([1],[[2]])	([1],[[0]])	
([1] [[0]])						
([1] [[1]])						
([1] [[2]])					([0],[[0]]	([0][[1]])

Osservazione G1,G2 abeliani ⇔ G1 x G2 abeliano
Esempio:
$S_3 \times Z_2 = \{(\sigma,[a]) | \sigma \in S_3, [a] \in Z_2\}$
Con operazione
$(\sigma,[a] ☆) (\tau,[b])=(\sigma \circ \tau,[a]+[b])$
$S_3=\{(1),(1\ 2),(1\ 3),(2\ 3),(1\ 2\ 3),(1\ 3\ 2)\}$
$Z_2=\{[o],[1]\}$
Per esempio
$((1\ 2),[1]) ☆ ((1\ 2\ 3),[1])=$
$=((1\ 2)\ (1\ 2\ 3),[1]+[1])=\{(2\ 3),[0])$

$((1\ 2\ 3\ ),\ [1])^{-1} =((1\ 2\ 3)^{-1},-1)=((1\ 3\ 2\ ),\ [1])$

Osservazione la costruzione si può generalizzare al prodotto diretto di 3 o più gruppi
(G1,☆1),(G2,☆2),(G3,☆)
(G1xG2xG3,☆) dove
(a,b,c)☆(a1,b1,c1)=(a☆a1,b☆2b1,c☆3c1)

Analogamente G1 x…….x Gn

Caso particolare

G x…x $g=g^n$

Per esempio
$Z^5\{(a,b,c,d,e)|\ a,b,c,d,e \in Z\}$
Con operazione componente per componente preso
=(7,3,0,-1,-1)+(2,-4,0,1,12)=(9,1,0,0,0,11)
Sottogruppi
esempi : Z è sottogruppo di Q
Q è sottogruppo di R,C

$Zn^{☆} \subseteq Zn$ ma $Zn^{☆}$ non è sottogruppo di Zn perché le operazioni di gruppo sono diverse

Definizione: sia (G,☆) un gruppo e H⊆G diciamo che H è un sottogruppo di G se:

a) H è stabile rispetto a ☆ cioè ∀x,y∈H,x☆y∈H
b) (H,☆) è un gruppo
   Esempi:
   -(Z,+) H=N
   N non è sottogruppo ((a)è soddisfatta ma (b) no)
   -(Z,+) H=2Z={2∩|∩∈Z} numeri pari
   H⊆2Z 2Z è sottogruppo 2Z<=Z
   H=1+2Z ={numero dispari} ⊆ Z
   H non <= Z (non è stabile rispetto a "+")

Proprietà sia H<=G ⇒

a) L'elemento neutro di H coincide con l'elemento di G
b) L'inverso di un elemento di H in H e in G coincidono

Criteri per determinare se H⊆G è un sottogruppo

Proposizione: sia G gruppo , $H \subseteq G$ allora $H \leq G \Leftrightarrow$

a) H è stabile rispetto all'operazione in G $a,b \in H \Rightarrow ab \in H$
b) $e_G \in H$
c) $\forall x \in H, x^{-1} \in H$

Esempio:

In Sn consideriamo

$A_n=\{\sigma \in S_n | \sigma \text{ pari}\}$(prodotto di un numero pari di trasposizioni)

Provo che $A_n \leq S_n$

a) È verificato:
   $\sigma,\tau \in A_n \Rightarrow \sigma \circ \tau$ è pari
b) $(1) \in A_n$ $(1)=(1\ 2)(1\ 2)$
c) Se $\sigma \in A_n \Rightarrow \sigma^{-1} \in A_n$
   $\sigma \in A_n \Rightarrow \sigma$ $(a_1b_1)(a_2b_2)....(a_k\ b_k)$k pari
   $\sigma^{-1} =(a_k\ b_k)(a_{k-1}\ b_{k-1})....(a_1\ b_1)$
   $\Rightarrow A_n \leq S_n$ sottogruppo alterno
   $|a_n|=n!/2$

Criterio dei sottogruppi

Sia G un gruppo e $H \subseteq G$

Allora $H \leq \Leftrightarrow$

1) $H \neq \emptyset$
2) $\forall x,y \in H$ $xy^{-1} \in H$

RIASSUNTO:	Scrivi qui il tuo riassunto:

Matematica discreta algebra geometría	Argomento trattato:
Lezione giovedì 03/12/2024	Esercizi e introduzione laterali (matematica discreta) prof. Lea Terracini
Domande e risposte / parole chiave ☰ = relazione di congruenza <= = sottogruppo ~ = tilde	Ripasso lezione precendente: sottogruppi : H<=G Proprietà: H⊆G è sottogruppo ⇔ a) H è stabile b) H contiene e c) X є H⇒x^{-1} є H Criterio dei sottogruppi H<=G ⇔ 1) H≠∅ 2) ∀x,yєH xy^{-1} єH Osservazione: Se G gruppo con elemento neutro e allora {e},G sono sottogruppi o Sottogruppi banali Proposizione: se H1,H2<=G allora H1∩H2<=G Dimostrazione: Applichiamo il criterio del sottogruppo 1)H1∩H2 ≠0 perchè e є H1 ∩ H2 2) supponiamo che x,y є H1 ∩ H2 x,y є H1 ⇒xy^{-1} є H1 X,y є H2⇒xy^{-1} є H2 quindi : xy^{-1} є H1∩H2 Esempio: 2Z<=Z

Analogamente $3Z<=Z$
$NZ<=Z \ \forall N \in N$
$2Z \cap 3Z=6Z$
$6z \cap 4z=12z$

$Nz \cap Mz=mz$
$m=mcm(n,m)$

In generale l’unione di sottogruppi non è sottogruppo
Es.
$2Z<=Z$, $3Z<=Z$
$2Z \cup 3Z$ non <= Z infatti $2 \in 2Z$, $3 \in 3Z$
Ma $2+3=5 \notin 2Z \cup 3Z$
$\Rightarrow 2Z \cup 3Z$ non è stabile rispetto alla somma
Quindi non è sotto gruppo

Proposizione: tutti i sottogruppi di Z sono tipo nZ per qualche $N \in N$

Esercizio:

1) In Q X Q si consideri la seguente operazione
   $(a,b)☆(c,d)=ac+7bd,ad+bc)$
   Dire se (QXQ) è gruppo
2) Sia $x=QxQ -\{(0,0)\}$
   Dimostrare che x è stabile rispetto a ☆ e dire se (x,☆) è gruppo

Soluzione:

Osserviamo che ☆ è commutativa
1) ☆ è associativa ?
   Cioè vale $(a,b)☆((c,d)☆(e,f))=((a,b)☆((c,d))☆(e,f))$ (cambiano le parentesi attenzione !!)

Calcoliamo il primo membro:
$(a,b)☆((c,d)☆(e,f))=$
$=(a,b)☆(ce+7df,cf+de)$
$=(a(ce+7df)+7b(cf+de),a(cf+de)+b(ce+7df)$
$Ace+7adf+7bcf+7bde$, $acf+ade+bce7\ 7bdf)$
Calcoliamo il secondo membro
$((a,b)☆((c,d))☆(e,f))$
$(ac+7bd*ad+bc)☆(ef)$
$=(ac+7bd)e+7(ad+bc)f(ac+7bd)f,+(ad+bc)e)$
$=ace+7bde+7adf+7bcf,acf+7bdf+ade+bce)$

I membri sono uguali quindi vale la proprietà associativa

b) esiste elemento neutro ?
Cioè esiste $(x,y) \in QxQ$ t.c. $\forall (a,b) \in QxQ$

Si abbia:
$(a,b)☆(x,y)=a,b)$
$(ax+7by7,ay+bx)=(a,b)$
Quindi devono valere
$ax+7by=a$
$ay+bx=b$

Osservo che ponendo a=1,b=0
Trovo x=1,y=0
Inoltre x=1,y=0 soddisfa (☆) per ogni (a,b)
⇒(1,0) è elemento neutro

c) è vero che ogni elemento in QxQ ha un inverso ?
cioè è vero che ∀(a,b) ϵ QxQ ∃(x,y) ϵ QxQ t.c (ab)☆(x,y)=1,0)

Cioè

$$\begin{cases} ax + 7by = 1 \\ bx + ay = 0 \end{cases}$$ non ha soluzioni se a=b=0 ((0,0) non è invertibile)
(QxQ,☆) non è gruppo

2) Verifichiamo che x è stabile rispetto ☆ (a,b),(c,d)ϵ x
   Cioè (a,b)≠(0,0) (c,d)≠(0,0)
   Si ha (a,b)☆(c,d)ϵ x
   Cioè (ac+7bd*ad+bc)≠(0,0)
   Consideriamo il sistema lineare omogeneo

$$\begin{cases} ac + 7bd = 0 \\ bc + ad = 0 \end{cases}$$

   Nelle incognite c,d
   La matrice dei coefficienti

$$\begin{bmatrix} a & 7b \\ b & a \end{bmatrix}$$

esiste soluzione non banale ⇔
Det $=a^2-7b^2=0$
   Ma se(a,b)≠(0,0)
   $a^2-7b^2=0 \Rightarrow (a/b)^2=7 \Rightarrow a/b=\pm\sqrt{7}$

Non può succedere se a,b ϵ Q
Quindi non esiste soluzione non banale
⇒ x è stabile
Per provare che (x,☆) è un gruppo basta provare che ogni (a,b)ϵ x è invertibile
Cioè se (a,b)≠(0,0) il sistema

$$\begin{cases} ax + 7by = 1 \\ bx + ay = 0 \end{cases}$$ ha soluzioni ?

Sistema lineare non omogeneo la matrice dei coefficienti è

$$\begin{bmatrix} a & 7b \\ b & a \end{bmatrix}$$

Ha det ≠ 0 quindi esiste soluzione ogni elemento è invertibile
(x,☆) è gruppo

Laterali (destri o sinistri) di un sottogruppo
G gruppo, H<=G
Definiamo su G due relazioni ~1 , ~2
Segue

	$X \sim 1\ y$ se $xy^{*-1}\ є\ H$ $X \sim 2\ y$ se $y^{*-1}\ є\ H$ Fatto: ~1 , ~2 sono relazioni di equivalenza su G Lo proviamo per ~1 proprietà riflessiva $x \sim 1\ x$ significa $xx^{-1} є\ H$ (xx^{-1} elemento neutro) Propietà simmetrica Supponiamo $x \sim 1y$ cioè $xy^{*-1}\ є\ H$ H sottogruppo quindi $(xy^{-1})^{-1}\ x^{-1}\ є\ H$ cioè $yx^{-1}\ є\ H$ $\Rightarrow y \sim 1x$ Proprietà transitiva Supponiamo $x \sim 1y$, $y \sim 1z$ Cioè $xy^{*-1}\ є\ H, yz^{*-1}\ є\ H$ H sottogruppo quindi $(xy^{-1})(yz^{-1}) є\ H$ Dato X є G denotiamo [x]1 la classe di x rispetto a ~1 [x]2 la classe di x rispetto a ~2 $[x]1=\{y\ є\ G\ \|yx^{-1}\ є\ H\}$ $=\{y\ є\ G\| \exists\ h\ є\ H$ t.c. $y=h*x\}$ $=\{hx\|hє\ H\}=h*x$ (laterali destri di H in G) analogamente $[x]2=\{y\ є\ G\ \|x^{-1}\ є\ H\}$ $=\{xh\|hє\ H\}=xh$ (laterali sinistri di H in G) Laterali destri = classi di equivalenza rispetto a ~1 Laterali sinistri = classi di equivalenza rispetto a ~2 Quindi $\forall$ x1,x2 є G X1 ~1 x2 ⇔ hx1=hx2 E X1 ~2 x2⇔ x1h=x2h

RIASSUNTO:	Scrivi qui il tuo riassunto:

—-

Matematica discreta algebra geometría	Argomento trattato:
Lezione giovedì 05/12/2024	I laterali ((matematica discreta) prof. Lea Terracini
Domande e risposte / parole chiave	Laterali: G gruppo H<=G Definisco su G due laterali

Ξ = relazione di congruenza	X~1 y se xy^{*-1} є H X~2 y se y^{*-1} є H Sono laterali di equivalenza su G Vediamo le loro classi di equivalenza: [x]1 classe di x rispetto a ~1 [x]2 classe di x rispetto a ~2 [x]1={hx|hє H }=h*x (laterali destri di H in G) [x]2={xh|hє H }=xh (laterali sinistri di H in G) Esempio: G=s3={(1),(1 2)(1 3),(2 3,(1 2 3),(1 3 2) h={(1),(1 2)}<=G Laterali destri di H in G H(1)={(1),(1 2)}=H=H(1 2) H(1 3)={(1)(1 3),(1 2) (1 3)}={(1 3),(1 3 2)} H(2 3)={(1)(2 3),(1 2)(2 3)}={(2 3),(1 2 3)} = H(1 2 3) Laterali sinistri H={(1)(1),(1)(1 2)}={(1),(1 2)}=H =(1 2)H (1 3)H={(1 3)(1),(1 3)(1 2)}={(1 3),(1 2 3)}=(1 2 3) (2 3)H ={(2 3)(1),(2 3)(1 2)} ={(2 3),(1 3 2)}=(1 3 2) H OSSERVAZIONE: H (1 3)≠ (1 3) H Laterali destri e sinistri non coincidono Esempio: (Z,+) H=NZ<=Z Z commutativo ⇒~1 e ~2 coincidono X~1 y se x-y є H =NZ Cioè se N/x-y Cioè se xΞ y mod N ⇒ le classi di equivalenza sono le classi di resto mod N Se xєZ il laterale (destro o sinistro) di NZ in Z rappresentato da x è: Hx NZ+x=[x]N Proposizione: Sia G gruppo H<=G Sia x є G la funzione Θ:H↦Hx h↦hx È bietttiva In particolare se G è finito e H<=G tutti i laterali (destri o sinistri) hanno la stessa cardinalità , uguale a |H| Teorema di lagrange : sia G un gruppo finito e H<=G allora |H|/|G| Se G gruppo finito |G|=ordine di G Lagrange: L'ordine di un sottogruppo divide l'ordine di un gruppo

Esempi:
G=Z7 |Z7|=7
Divisori di 7: 1,7
Z7 ha come unici sottogruppi i gruppi banali {[0]7}z7
(vale per ogni Zp con p primo

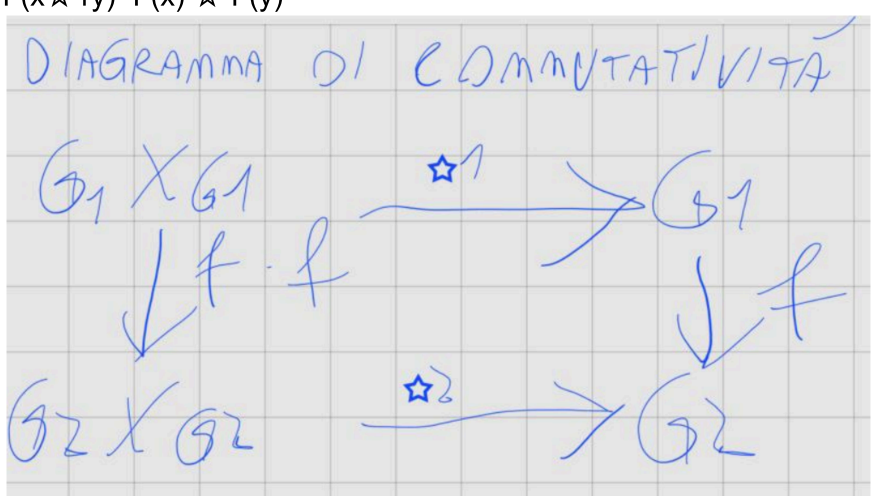
Z4 |Z4|=4
Divisori di 4 sono : 1 , 2 , 4
{[0]4}→ordine 1
{[0],[2]}→ordine 2
{[0],[1],[2],[3]}=z4 ordine 4

S4 ordine |S4|=4! = 24
Divisori di 24: 1,2,3,4,6,8,12,24
S4 non ha sottogruppi di ordine 5x24
H={(1),(1 2),(3 4),(1 2 3 4),(1 2 3)}
Non è sottogruppo (per lagrange (condizione cartesiana))
S4 ha un sottogruppo di ordine 12:A4

|A4|=12 divisori di 12 : 1,2,3,4,6,12
Per lagrange tutti i sottogruppi di A4 hanno ordine uguale ad un divisore di 12
Si può provare che A4 non ha sottogruppo di ordine 6
⇒il teorema di lagrange non si inverte non è vero in generale che se |G|=n e d/n G ha sottogruppo di ordine d
(è vero però per gruppi abeliani)

---

omomorfismo
Definizione: siano (G1,☆1)(g2,☆2) gruppi un omomorfismo è una funzione F G1→G2
t.c. ∀ x, y є G1
F(x☆1y)=F(x) ☆ F(y)



Esempi:
-F: Z→Z
 K→3K
È un omomorfismo
F(k1+k2)= 3(k1+k2)
F(k1)+f(k2)=3k1+3k2

∀ gruppo G
F:G→G

$X \to e$ è omomorfismo banale

$F: Z \to R$
$K \to k^2$ non è un omomorfismo

$F(k1+k2)=(k1+k2)^2 \neq F(k1)+F(k2)$
$=k1^2+k2^2$

Id: $G \to G$ è omomorfismo
E se $H<=G$
$i:H \to G$
$X \to x$ è omomorfismo

Funzione esponenziale
$R \to R^{\star}$
$X \to e^{\star}$ è omomorfismo $\exp(x+y)=e^{x+y}=e^y = \exp(x) \exp(y)$

LOG $R \to R$
$X \mapsto$ LOG(X) È OMOMORFISMO
$\log(X Y) = \log(X) + \log(Y)$

$- \pi : Z \to Z_n$
$a \mapsto [a]_n$
OMOMORFISMO PERCHÈ:
$\pi(a+b) = [a+b]_n$
$\pi(a) + \pi(b) = [a]_n + [b]_n$

$- f : S_n \to \{\pm 1\}$ → SOTTOGRUPPO DI $R^{\star}$
$\sigma \mapsto$ SEGNO(σ)

$$\sigma \mapsto \text{SEGNO}(\sigma) = \begin{cases} 1 & \text{SE } \sigma \text{ PARI} \\ -1 & \text{SE } \sigma \text{ DISPARI} \end{cases}$$

sg (SEGNO) È OMOMORFISMO

$$sg(\sigma \circ \mu) = sg(\sigma)\, sg(\mu)$$

sg	σ	μ	$\sigma \circ \mu$
	1	1	1
	1	−1	−1
	−1	1	−1
	−1	−1	1

PROP: SIA G_1, G_2 GRUPPI

E $f : G_1 \to G_2$ OMOMORFISMO

$$\left(f(\underset{\text{IN } G_1}{x\,y}) = f(x) \underset{\text{OPPOSTO IN } G_2}{\,} f(y)\right)$$

ALLORA

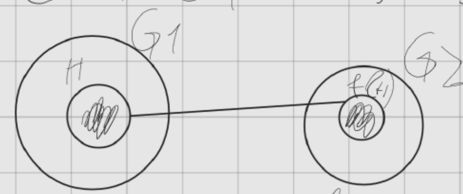
1) $f(e_{G_1}) = e_{G_2}$

2) $\forall x \in G_1 \quad f(x^{-1}) = f(x)^{-1}$

3) $\forall x \in G_1$ e $\forall n \in \mathbb{Z} \quad f(x^n) = f(x)^n$

INOLTRE

4) SE $H \leq G_1$ ALLORA $f(H) \leq G_2$



$\{f(h) \mid h \in H\}$

5) SE $K \leq G_2$ ALLORA $f^{-1}(K) \leq G_1$

$(f^{-1}(K) = \{x \in G_1 \mid f(x) \in K\}$

Cioè immagini e controimmagini di sottogruppi mediante omomorfismi sono sottogruppi

RIASSUNTO:	Scrivi qui il tuo riassunto:

—

Matematica discreta algebra geometría	Argomento trattato:
Lezione giovedì 06/12/2024	Omomorfismi ((matematica discreta) prof. Lea Terracini
Domande e risposte / parole chiave 三 = relazione di congruenza	G1,G2 gruppi F:G1→G omomorfismo se ∀ x,y ∈ G1 F:(x y)=F(x)F(y) Proprietà:

PROP: SIA G1, G2 GRUPPI

E $f: G1 \to G2$ OMOMORFISMO

$(f(x \cdot y) = f(x) f(y))$

IN G1 — OPPOSTO IN G2

ALLORA

1) $f(e_{G1}) = e_{G2}$

2) $\forall x \in G1 \; f(x^{-1}) = f(x)^{-1}$

3) $\forall x \in G1 \; \& \; \forall m \in \mathbb{Z} \; f(x^m) = f(x)^m$

INOLTRE

4) SE $H \leq G1$ ALLORA $f(H) \leq G2$

$\{f(h) \mid h \in H\}$

5) SE $K \leq G2$ ALLORA $f^{-1}(K) \leq G1$

$(f^{-1}(K) = \{x \in G1 \mid f(x) \in K\})$

Casi notevoli:
-se H=G1 , allora F(g1)= im(immagine) F <=G2
⇒l'immagine di un omomorfismo è sottogruppo
-consideriamo k={eG2}<=G2
F^{-1}(k)={x ∈ G1 | F(x)=eG2}<=G1
Il nucleo (ker) e l'immagine di un omomorfismo sono sottogruppi
Esempi:
-π:z→zN omomorfismo(di gruppi)
a→[a]n
π è suriettiva: ogni elemento di Zn è del tipo [a]n per qualche a , quindi è π(a) immagine π=Zn
Ker π={a є Z|π(a)=[0]n}
={a є Z|a☰0 mod n }
={a є Z|N{a}=NZ

-Segno: sn→{+-1} funzione segno (suriettiva) omomorfismo

Segno è suriettiva se >= 2 quindi immagine del segno={+-1}
Ker sg={σ є Sn|sg(σ)=1}
Ovvero sottogruppo alterno di Sn (An<=Sn)

Esponenziale:
$R \to R^{☆}$ funzione esponenziale omomorfismo
$x \to e^{x}$
In exp $R^{☆}$ >0 {x є R|x>0}<=$R^{☆}$
Ker exp= {x є R| e^{x} =1}={0}

Terminologia:

F:G1→G2 omomorfismo si dice:

-monomorfismo se è iniettivo
-epimorfismo se è surriettivo
-isomorfismo se è biettivo
-endomorfismo se G1=G2
-automorfismo se G1=G2 ed è biettivo

proposizione : F:G1→G2 omomorfismo
F iniettivo ⇔ ker F={eG1} (e elemento neutro)

Esempi:
π:z→zN N>=2
a→[x]
Ker F= NZ ≠{0}⇒π non è iniettiva
sg:Sn→{+-1}
(non è iniettiva se n>=3 perchè |Sn|=n!>2)
Ker sg sg0 An ≠ {(1)}se n>=B
-exp:$R \to R^{☆}$ ha ker={0}
-F:Z→Z N є N
a→Na
endomorfismo
Im F=nz 1){0} se N=0
2)Nz(sotto gruppo proprio non banale)
3)Z se N=1

Ker F= 1) Z se N=0
2){0} se N≠0
F iniettiva ⇔ N≠0
F suriettiva ⇔ N=1
F biettiva ⇔ N=1

(in C oni polinomio ammette soluzione)
-G:$R^{☆} \to R^{☆}$
$x \to x^{5}$
G omomorfismo: se x,y є$R^{☆}$
G(x y)=$(x\ y)^{5}$ =xy*xy*xy*xy*xy=x^{5}*y^{5}
G(x) G(y)=$x^{5}y^{5}$
Perché $R^{☆}$ è commutativo
G è biettiva allora è automorfismo di $R^{☆}$

-considero ora:
h:C☆→C☆
z→z^5
H omomorfismo perchè C☆ commutativo
ker h={Z є C| Z^5 =1}
={radici del polinomio x^5-1}
={1,Z1,Z2,Z3,Z4}
Dove:
Zk= cos 2kπ/5 + i suoi 2kπ/5 k=1…4
→h non è iniettiva
h è surriettiva ?
Im h ={Z| ∃ W є C☆ t.c. w^5=Z}
={Z|il polinomio x^5-Z ha radice }
= C☆ perchè in C ogni polinomio non costante ha una radice

---

isomorfismi :
Def: due gruppi G1,G2 si dicono isomorfi se esiste un isomorfismo F:G1→G2 (in questo caso F^{-1}:G1→G2 isomorfismo)
Due gruppi isomorfi sono "moralmente" lo stesso gruppo ovvero hanno le stesse proprietà
G1 finito ⇔ G2 finito
G1 abeliano ⇔ G2 abeliano
G1 ciclico ⇔ G2 ciclico

Esempio importante!!!!!
Supponiamo m,n є N m,n>=2 t.c. n/m
Consideriamo la funzione:
F:Zm→Zn
[a]m→[a]n
È ben definita se non dipende dalla scelta del rappresentante cioè:
Se [a]m=[a^1],⇒[a]n=[a^1]n
Nota bene è essenziale che n/m

Se n/m:
Esempio:
m=45 n=9
F:Z45→Z9
[a]45 →[a]9
Ker F={[a]45|[a]9=[0]9}
={[a]45|9/a}
={[0]45,[9]45,[18]45,[27]45,[36]45}(tutti i multipli di 9 fino a 45)

Variante n/m
G: Zm☆→Zn☆
[a]m→[a]n
G è ben definita perchè se:
[a]m є Zm☆⇔(a,m)=1(coprimo)
⇒(a,m)=1
⇒[a]n є Zn☆

G omomorfismo infatti:
g([a]m[b]m)=g([ab]n)=[ab]n=g([a]m)g([b]m)

Si dimostra che g è suriettiva
m=45 n=9
Ker G={[a]45 є Z45☆/[a]9=[1]9}
={[a]45 є Z45☆|a☰1 mod 9}
={[1]45,[19]45 [28]45, [37]45}
G non è iniettiva perchè ker G ≠{{1]45}

Gruppi ciclici:
Sia G gruppo x є G
H={x^n|n є Z} <= G
H<=G infatti (criterio dei sottogruppi)
1)H≠Ø
2) se x^n, x^m є H allora
$x^n(x^m)^{-1} = x^n, x^{-m}=x^{n-m}$ є H
H si dice sottogruppo ciclico generato da X =<x>

Esempio
-in S5 consideriamo
<(1 2 3)>={$(1\ 2\ 3)^n$|n є Z}
={(1),(1 2 3),(1 3 2)}
-in Z consideriamo
<3>={3n|n є Z}=3z

In Z19☆ consideriamo
<[2]>={[1],[2],[4],[8],[16,[13],[7],[14],[9],[18],[17].[15],[11],[3],[6],[12].[5],[10]}
|Z19☆|= φ(19)=19-1=18 (cardinalità)

Verificare che anche <[13]>=Z19☆

Z13*

$\langle \overline{13} \rangle = \{\overline{1}, \overline{13}, \overline{7}, \overline{14}, \overline{3}, \overline{15}, \overline{9}, \overline{3}, \overline{16}, \overline{10}, \overline{4}, \overline{17}, \overline{11}, \overline{5}, \overline{18}, \overline{12}, \overline{6}, \overline{13}\}$

Def: se G è un gruppo ed esiste X є G t.c.
<x>=G allora G si dice gruppo ciclico e x si dice generatore di G
Quindi Z19☆ è un esempio di gruppo ciclico
[2] è generatore
[13] è generatore

RIASSUNTO:	Scrivi qui il tuo riassunto:

—

Matematica discreta algebra geometría	Argomento trattato:
Lezione giovedì 12/12/2024	Ciclicità dei gruppi prodotto((matematica discreta) prof. Lea Terracini
Domande e risposte / parole chiave 三 = relazione di congruenza	Non è detto che il prodotto diretto di gruppi ciclici sia ciclico. Ciclicità dei gruppi prodotto G1,G2 gruppi ciclici ⇔ G1, G2 sono finiti e hanno ordini coprimi.

Funzione di eulero è moltiplicativa cioè (m,n)=1 $\varphi(mn)=\varphi(m)\varphi(n)$
Sappiamo che p primo
$\varphi(p^e)=p^{e-1}(p-1)$

Esempio:
$\varphi(5985)$
1)Scomposizione in fattori
$5985=3^2*5*11^3$
$\varphi(5985)=\varphi(3^2)\varphi(5)\varphi(11^3)$
$=3(3-1)*(5-1)11^2(11-1)$
$=3*2*4*121*10=29040$
Applicazione del teorema di eulero al di potenze di mod N
Teorema di eulero:
se (a,N)=1 allora $a^{\varphi(n)}\equiv 1 \bmod n$

Esempio:
Calcolare il resto della divisione per 29 di 3^{12007}
Soluzione:
Calcolare il rappresentante canonico di $[3]^{12007}{}_{29}$
Osserviamo che (3,29)=1
$\Rightarrow$eulero $3^1\equiv 1 \bmod 29$
$\varphi(29)=28$ (cardinalità)
$3^{28}\equiv 1 \bmod 29$
Dividiamo 12007 per 28
12007=28*428+23
$3^{12007}=3^{28*428}+3^{23}$
$(3^{28})^{428}\equiv 1 \bmod 29$
$1*3^{23} \bmod 29$
Osservo che $3^3\equiv -2 \bmod 29$
$3^{23}=3^{3*7}*3^2\equiv(-2)^7*9 \bmod 29$
$\equiv -128*9 \bmod 29$
$\equiv -12*9 \bmod 29$
$\equiv -21 \bmod 29$
$\equiv 8 \bmod 29$
Quindi il resto richiesto è 8
Attenzione il teorema di eulero si può applicare solo se (a,n)=1

Esercizio:
Calcolare il resto della divisione per 30 di
$2^{141232}+7^{6536779}$
Sol:
a=141232 b=6536779
Stiamo cercando il rappresentante canonico
Di $[2^a+7^b]_3$ $[2^a]_{30}+[7^b]_{30}$
Sonsidero 7^b
mcd(7,30)=1
eulero : $7^{\varphi(30)}\equiv 1 \bmod 30$
$\varphi(30)=\varphi(2)\varphi(3)\varphi(5)$ (30=2*3*5)
=1*2*4=8
$7^8\equiv 1 \bmod 30$

Dividiamo b per c e consideriamo il resto
$B\equiv 3 \bmod 8$ b=8k+3
Ne segue
$7^b=7^{8k} * 7^3 =(7^8)^k * 7^3 \bmod 30$

$[7^b]_{30} = [7^3]_{30} = [19*7]_{30} = [343]_{30} = [13]_{30}$

Considero 2^a eulero non è applicabile

Scrivo le potenze di [2] in Z30
$[2]^0 = [1]$ $[2]^1 = [2]$ $[2]^2 = [4]$ $[2]^3 = [8]$ $[2]^4 = [16]$ $[2]^5 = [32] = [2]$
$[2]^6 = [4]$ $[2]^7 = [8]$ $[2]^8 = [16]$ $[2]^9 = [2]$

Vediamo che s>=1
$[2]^s$ = 1) [2] se s☰1 mod 4
2) [4] se s☰2 mod 4
3) [8] se s☰3 mod 4
4) [16] se s☰4 mod 4

Ho a=141232 mod 34

⇒2^a☰16 mod 30 $[2^a]_{30} = [16]_{30}$
Otteniamo

$[2^a]_{30} + [7^b]_{30} = [16]_{30} + [13]_{30} = [29]_{30}$

29 è il resto richiesto

Congruenza:

Una congruenza è un equazione della forma ax☰b mod n
Con a,b,n є Z, n>=2

Risolvere la congruenza = a trovare tutti i valori di x che ci danno soluzione

Osservazione: non è detto che ci siano soluzioni.

Per esempio 3x☰1 mod 6
Non ha soluzioni perchè altrimenti 3 є $Z_6^{\star}$

2) se c'è una soluzione X0 allora per ogni y se y☰x0 mod N anxhe y è soluzuone
allora : tutti gli elementi in [x0]n sono soluzioni

Allora o non ci sono soluzioni o le soluzioni sono infinite
Quando una congruenza ha soluzioni?
Ax0☰b mod n se solo se esiste y appartente a Z t.c.
ax0+ny0=b

Quindi:
Ax☰b mod n ha soluzioni se solo se: l'equazione ax+ny=b ha soluzione

Se e solo se (a,n) divide b

Come trovare tutte le soluzioni?

Esempio: 4x☰2 mod 6
Ha soluzione perchè (4,6)(mcd)=2 divide 2

Per determinare le soluzioni divido per 2 e ottengo 2xΞ1 mod 3
Cerco $[2]^{-1}_{3}=[2]_{3}$

Moltiplico la congruenza per il risultato
2*2xΞ2 mod 3
XΞ2 mod 3

Le soluzioni mod 6 sono
XΞ2 mod 6 , xΞ5 mod 6
Cioè $[2]_{6}$ o $[5]_{6}$

Regola generale:

Data la congruenza
AxΞb mod n

1) Calcolo d=(a,n)
   Se d ∤ b non ci sono soluzioni
   Se d/b ci sono soluzioni

   In questo caso cerco le soluzioni pongo a1xΞb1 mod n1n

   Si ha (a1,n1)=1 allora a1 invertibile mod n1

   Bèzout calcolo $[a1]^{-1}_{n1}=[c]_{n1}$
   Moltiplico per c primo e secondo membro in a1xΞb1 mod n1n
   XΞcb1 mod n1 pongo s=cb1

   Modulo n le soluzioni sono:
   XΞs mod n
   x=s+n1 mod n
   XΞs+2 n1 mod n
   ……….
   xΞs+(d-1)n1 mod n

   Cioè
   $[s]_{n1}$ $[s+n1]_{n}$ $[s+2n1]_{n}$….$[s+(d-1)n1]_{n}$

   Ci sono classi di resto mod n che sono soluzioni

Esempio:

Elencare le soluzioni in Z68 della congruenza 12xΞ8 mod 68

Soluzione:

mcd(12,68)=4 divide 8= ci sono soluzioni

Troviamole:

Divido per 4 trovo congruenza

3xΞ2 mod 17

Cerco $[3]^{-1}_{17}$

Bezout

17=5*3+2
3=2+1

1=3*2=3-(17-5*3)=6*3-17

$[3]^{-1}_{17} = [6]_{17}$

Moltiplico 3x三2 mod 17 per 6

6*3x三2*6 mod 17

Le soluzioni in Z68 sono:

[12],[12+17] [12+17] [12+34] [12+51]

Ovvero
[12] [29] [46] [63]

Scrivi qui il tuo riassunto: