ALGEBRA (M-Z)

(2013-14)

SCHEDA 3

Strutture algebriche

1.STRUTTURE ALGEBRICHE

Sia (M,•) *un monoide con unità* 1_M *e sia* $a \in M$. Le ***iterazioni della operazione*** . sono definite da:

$$a^0 = 1_M,\ a^{n+1} = a \bullet a^n.$$

1.1.Dimostrare che $a^m \bullet a^n = a^{m+n}$ e $(a^m)^n = a^{mn}$.

1.2. Sia (M,•) un monoide e sia $a \in M$. Dimostrare che esiste un solo morfismo di monoidi $f : (\mathbf{N},+) \to (M,\bullet)$ tale che $f(1) = a$.

1.3. Siano (A,·) e (A',•) strutture algebriche e sia f: A→A' un morfismo, ossia:

$$f(a \cdot b) = f(a) \bullet f(b) \text{ per ogni } a,b \in A$$

dimostrare che $(A/\sim_f,\cdot)$, dove $\sim_f$ è la relazione individuata da f, è una struttura algebrica isomorfa ad (A',•).

1.2. . Siano (A,·) e (A',•) strutture algebriche. Dimostrare che la composta di morfismi e l'inversa di un morfismo sono morfismi.

2.GRUPPI.

2.1. Determinare quali delle seguenti strutture algebriche (A,·) sono monoidi e quali gruppi:

- A= Z, con $a \cdot b = a - b$.
- A = Z-{0}, con l'usuale prodotto.
- A= {p/q∈Q : MCD(p,q) =1 q è dispari},con $a \cdot b = a + b$.
- A= {0,1,2,3,4 } $a \cdot b$ = resto della divisione per 5 di $a+b$.
- A={0,1,2,3,4 } $a \cdot b$ = resto della divisione per 5 di *a per b*.
- A = {1,2,3,4,5} $a \cdot b$ = resto della divisione per 6 di *a per b.*

2.2. Sia (G,·) un gruppo. Verificare che l'insieme degli automorfismi f :G→G è un gruppo rispetto alla composizione di funzioni. Tale gruppo sarà indicato con Aut(G) e si chiama anche ***gruppo delle trasformazioni di*** G.

2.3. Dimostrare che in un gruppo (G,·) valgono le leggi di cancellazione a sinistra : $g \cdot h = g \cdot k$ implica h = k; e a destra: $h \cdot g = k \cdot g$ implica h = k.

2.4. Dimostrare che se (G,·) è una struttura algebrica associativa tale che:

- G è finito,

- in G valgono le leggi di cancellazione.

  Allora (G,·) è un gruppo. (cfr. "Algebra Moderna"pag. 61)

2.4. Sia (G,·) un gruppo. Un sottoinsieme S non vuoto di G è un sottogruppo se e solo se per ogni $s,t \in S$ si ha: $s \cdot t^{-1} \in S$.

2.5. Sia E un insieme e sia A un suo sottoinsieme non vuoto. Posto:

$$G(A) = \{f \in S(E) : f(a) = a, \text{ per ogni } a \text{ di } A\}$$

dimostrare che G(A) è un sottogruppo di S(E). (cfr."Algebra Moderna"pag. 53)

2.6. Sia *n* un numero intero maggiore di 1. Verificare che l'insieme dei multipli interi di *n* è un sottogruppo di Z.

2.7. Sia $Q = \{1,-1,i,-i,j,-j,k,-k\}$ con l'operazione · definita da:

$$i^2, j^2, k^2 = -1, i \cdot j = k$$

è un gruppo chiamato *gruppo dei quaternioni.* Determinare tutti i sottogruppi di tale gruppo. (cfr. "Algebra moderna" pag. 51). Scrivere la tabella di composizione.

2.8. Siano (G,·) un gruppo e X un insieme non vuoto, definire una struttura di gruppo nell'insieme G^X delle applicazioni da X in G.

2.9. Siano (G,·) e (H,*) gruppi, definire una struttura di gruppo nell'insieme prodotto GxH.

2.10. Sia (G,·) un gruppo finito dimostrare che un sottoinsieme non vuoto T di G è un sottogruppo se e solo se T è chiuso.

2.11. Si consideri in **Q** l'operazione * definita ponendo x*y = 3xy/2. Che tipo di struttura è (**Q**,*)?

2.12. Dato un gruppo (G,·) e un elemento *g* di G dimostrare che esiste un solo morfismo di gruppi f: (**Z**,+) → (G,·) tale $f(1) = g$.

2.13. Sia f: (G,·) → (H,·) un morfismo di gruppi dimostrare che se T è un sottogruppo di G allora f(T) è un sottogruppo di H.

2.14. Si consideri in **Q** l'operazione * definita ponendo x*y = (x+y)-1/3. Che tipo di struttura è (**Q**,*)?

2.15. Si consideri la struttura algebrica (2**Z**,*) dove 2**Z** è l'insieme dei numeri pari e * è l'operazione su 2**Z** definita da z*w = 4z+4w-zw/2 -24. Si provi che tale struttura è un gruppo. Si consideri l'applicazione f :(**Z**,·) → (2**Z**,*) definita ponendo f(x) = 8-2x. Verificare che f è un isomorfismo di gruppi, ossia :

- f è biunivoca,
- f è un morfismo di gruppi.

2.16. Dimostrare che se H e T sono sottogruppi del gruppo (G,·) allora H∩T è un sottogruppo di G.

2.17. Sia X = {a,b,c}. Si consideri la struttura algebrica (X,*) dove * è definita dalla seguente tavola di composizione:

*	a	b	c
a	a	b	C
b	b	c	a
c	c	a	b

Quali sono le proprietà di *? Che tipo di struttura algebrica è (X,*)?

2.18. Sia E un insieme e sia A un suo sottoinsieme non vuoto. Posto:

$$G(A) = \{f \in S(E) : f(A) = A\}$$

dimostrare che G(A) è un sottogruppo di S(E).

3.ANELLO **K**[x] DEI POLINOMI NELL'INDETERMINATA x.

3.1. Dimostrare che gli unici polinomi invertibili sono i polinomi di grado zero.

3.2. Siano $f(x)$ e $g(x)$ polinomi con $g(x) \neq 0$. Dimostrare per induzione sul grado di $f(x)$ che esiste un'unica coppia di polinomi $(q(x),r(x))$ tale che:

i) $f(x) = g(x)q(x) + r(x)$

ii) $r(x) = 0$ oppure $\deg r(x) < \deg g(x)$.

Un elemento $c \in$ **K** *si dice* ***radice*** *del polinomio* $f(x)$ *se risulta* $f(c) = 0$.

3.3. Dimostrare che c è radice di $f(x)$ se e solo se il polinomio $(x-c)$ divide $f(x)$, ossia $f(x) = g(x)(x-c)$.

3.4. Dimostrare che un polinomio di grado n ha al più n radici.

3.5. Posto **K** = Z_7 determinare le radici dei polinomi : $x^2 -1$, $x^2-3x +2$, $2x^2-x+1$. Questi polinomi sono divisibili per (x-1)?

3.6. In $Z_{11}[x]$ si considerino i polinomi $f(x) = x^8-2x^5+4x^3+6x-10$ e $g(x) = 8x^3+10x+2$. Si determinino i polinomi: $f(x) + g(x)$ e $f(x)g(x)$.

3.7. Posto **K** = Z_p con p numero primo, si verifichi che nè 1 nè 5 sono radici di $g(x) = x^2-6x+4$. Si determinino i valori di p per i quali 10 è radice di $g(x)$ e i valori di p per i quali $g(x)$ ha radice doppia.

3.8. Posto **K** = Z_5, determinare i valori di a affinchè il polinomio (x^4+ax+a) abbia radici.

3.9. Siano $f(x)$ e $g(x)$ polinomi di **R**[x]. Dimostrare che $f(x) = g(x)$ se e solo se per ogni $n \in N$ si ha: $f(n) = g(n)$.

3.10. Sia **K** un campo. Si indichi con **K**(x) l'insieme delle endofunzioni polinomiali di **K**, ossia:

K(x) = $\{f \in \mathbf{K}^K$: esiste un polinomio $p(x) \in$ **K**[x] tale che $f(k) = p(k)$, per ogni $k \in$ **K**$\}$.

Verificare che **K**(x) è un sottoanello dell'anello $(\mathbf{K}^K,+,.)$ con le operazioni naturali.

Si osservi che due polinomi distinti possono individuare la stessa funzione polinomiale. Si dimostri che se **K** è un campo con infiniti elementi allora due polinomi che individuano la stessa funzione polinomiale sono uguali.

4.L'ANELLO DEGLI INTERI,ALGORITMO DI EUCLIDE, MCD(a,b), CLASSI RESTO MODULO N.

4.1. Usando l'algoritmo euclideo delle divisioni successive, determinare il massimo

comun divisore di a e b ed esprimerlo nella forma as+bt con s,t interi (identità di Bézout), quando:
a = -1705 e b = 325
a = -1605 e b = -738
a = 2094 e b = 18
a = 5305 e b = 9150
4.2. Verificare che MCD(a,b) = MCD(a,b+ax) per ogni intero x.
4.3. Dimostrare per induzione il teorema fondamentale dell'aritmetica: ogni numero naturale n ≥ 2 si esprime come prodotto di numeri primi.
4.4. Siano $a,b,c \geq 1$ e tali che a/bc. Dimostrare che se MCD(a,b) = 1 allora a divide c. Quindi se p è un numero primo e p/ab allora p divide a oppure b.
4.5. Siano m e n interi maggiori di 1 e sia

$$A = \{p \in \mathbf{N} : p \text{ è primo e } p/m \text{ oppure } p/n\} = \{p_1, \ldots, p_t\}$$

pertanto:

$$m = p_1^{a(1)} p_2^{a(2)} \ldots p_t^{a(t)} \quad \text{e} \quad n = p_1^{b(1)} p_2^{b(2)} \ldots p_t^{b(t)}$$

Completare le seguenti frasi:

a) m divide n se.....
b) Il massimo comun divisore di m ed n è.....
c) Il minimo comune multiplo di m ed n è....
d) m/n è un intero se ....
e) m/n è un intero divisibile per p_i se ...

4.6. Dimostrare che:
a) Se MCD(a,b) = 1 allora mcm(a,b) = ab.
b) mcm(ka,kb) = k mcm(a,b).
c) Se d =MCD(a,b) allora MCD(a/d, b/d) =1.
d) mcm(a,b) = ab /MCD(a,b)
4.7.Verificare la compatibilità delle seguenti congruenze e quando possibile determinare le soluzioni:
12x ≡ 7 mod 21, 12x ≡ 7 mod 84, 12x ≡ 7 mod 73, 12x ≡ 7 mod 46,12x ≡ 7 mod 35.
4.8. Determinare gli elementi invertibili e i rispettivi inversi di $\mathbf{Z}_6$,$\mathbf{Z}_8$,$\mathbf{Z}_{10}$ $\mathbf{Z}_{11}$.
4.9. Scrivere la tabella di addizione e moltiplicazione per ($\mathbf{Z}_2 x \mathbf{Z}_3$,+, •) dove + e • sono le operazioni naturali definite da:
$([a]_2,[b]_3) + ([c]_2,[d]_3) = ([a]_2,+[c]_2,[b]_3+[d]_3)$
$([a]_2,[b]_3) \bullet ([c]_2,[d]_3) = ([a]_2[c]_2,[b]_3[d]_3)$
Che tipo di struttura è ($\mathbf{Z}_2 x \mathbf{Z}_3$,+, •)? Quali sono gli elementi invertibili?
Sia $f : \mathbf{Z_6} \rightarrow \mathbf{Z}_2 x \mathbf{Z}_3$ l'applicazione definita da $f([x]_6) = ([x]_2,[x]_3)$ verificare che f è biettiva, $\mathbf{Z_6}$ e ($\mathbf{Z}_2 x \mathbf{Z}_3$,+, •) sono isomorfi?
4.10. Sia a un numero espresso in base 10 da: $a = a_n 10^n + a_{n-1} 10^{n-1} + \ldots a_1 10 + a_0$. Dimostrare i criteri di divisibilità:
9 divide a se e solo se 9 divide la somma delle cifre $a_n + a_{n-1} + \ldots a_1 + a_0$ -
3 divide a se e solo se 3 divide la somma delle cifre $a_n + a_{n-1} + \ldots a_1 + a_0$ -

5 divide a se e solo se 5 divide a_0 .
11 divide a se e solo se 11 divide $a_0 - a_1 + a_2 - ... + (-1)^n a_n$
4.11. Dimostrare usando il teorema fondamentale dell'aritmetica che se p è un numero primo allora $\sqrt{p}$ è un numero irrazionale.
4.12**.** Dimostrare che $n(n+1)(2n+1) \equiv 0 \bmod 6$.
4.13**.** Verificare se sono isomorfi i gruppi $u(\mathbf{Z}_5)$, $u(\mathbf{Z}_8)$, $u(\mathbf{Z}_{10})$ degli elementi invertibili rispettivamente di $\mathbf{Z}_5$, $\mathbf{Z}_8$,$\mathbf{Z}_{10}$. Quali sono isomorfi al gruppo $(\mathbf{Z}_4,+)$?

5.PERMUTAZIONI

5.1.Esprimere le seguenti permutazioni rappresentate da una parola come prodotto di cicli disgiunti: $\sigma_1 = 537824169$, $\sigma_2 = 935128746$, $\sigma_3 = 524983176$,$\sigma_4 = 736892154$. Rappresentarle in forma standard come prodotto di cicli.
5.2. Verificare se σ è una permutazione di S_n esiste k in **N** non nullo tale che $\sigma^k = 1$, il più piccolo di tali interi si dice ordine di σ. Dimostrare che l'ordine di una permutazione e il minimo comune multiplo delle lunghezze dei suoi cicli.
5.3. Sia $\sigma \in S_n$, verificare che due cicli disgiunti di σ commutano.
5.4. Determinare la parità delle permutazioni in 5.1. ed esprimerle come prodotto di trasposizioni.
5.5. Verificare che se σ è una permutazione di S_n di classe dispari, allora per ogni permutazione τ si ha $\tau^2 \neq \sigma$.
5.6.Dimostrare che ogni permutazione è il prodotto di permutazioni 3-cicliche.
5.7.Dimostrare che se X ed Y sono insiemi equipotenti allora l'insieme S(X) delle permutazioni di X è equipotente all'insieme S(Y) delle permutazioni di Y.
5.8.Dimostrare l'insieme A_n delle permutazioni pari è un sottogruppo del gruppo simmetrico S_n. di cardinalità n!/2.