Corso di Laurea in Informatica - AA 2018-19

ALGEBRA

Prova scritta - I appello sessione

11 gennaio 2019

Antonietta Venezia (Canale Pb-Z)

Svolgere gli esercizi esplicitando il percorso logico seguito per giungere alla soluzione. Non è permesso consultare appunti e testi.

Soluzioni

Parte I

ESERCIZIO 1.1. Dati i numeri $m = 7007$ e $n = 1991$, determinare :

a) il MCD(7007, 1991) mediante l'algoritmo di Euclide,
b) una identità di Bézout,
c) le soluzioni, se possibile, dell'equazione in $\mathbf{Z}_{7007}$: $1991x = 44$.

Sol. L'algoritmo di Euclide applicato ai numeri 7007 e 1991 è il seguente:

$7007 = 1991(3) + \underline{1034}$ — $\underline{1034} = 7007 - 1991(3)$
$1991 = 1034 + \underline{957}$ — $\underline{957} = 1991 - 1034$
$1034 = 957 + \underline{77}$ — $\underline{77} = 1034 - 957$
$957 = 77\,(12) + \underline{33}$ — $\underline{33} = 957 - 77(12)$
$77 = 33(2) + \underline{11}$ — $\underline{11} = 77 - 33(2)$
$33 = 11(3)$

Pertanto il MCD(7007,1991) = 11, essendo questo l'ultimo resto non zero. Una identità di Bézout si ottiene nel seguente modo:

$11 = 77 - 33(2) = 77 - \big(957 - 77(12)\big)(2) = 77(25) - 957(2) =$
$= (1034 - 957)(25) - 957(2) = 1034(25) - 957(27) = 1034(25) - (1991 - 1034)(27) =$
$= 1034(52) - 1991(27) = (7007 - 1991(3))(52) - 1991(27) = 7007(52) - 1991(183).$

Pertanto una identità di Bézout è $11 = 7007(52) + 1991(-183)$.

L'equazione in $\mathbf{Z}_{7007}$: $1991x = 44$ ha soluzione in quanto MCD(7007,1991) = 11 divide 44. In $\mathbf{Z}_{637}$, l'equazione: $181x = 4$ ha una sola soluzione data da : $x = 181^{-1}4 = 1816 = 542$. Infatti dalla identità di Bézout:

$$1 = 637(52) + 181(-183),$$

si ricava che l'inverso di 181 in $\mathbf{Z}_{637}$ è 454.

Pertanto in $\mathbf{Z}_{7007}$ le soluzioni dell'equazione data sono 11: 542, 542+637, 542+ (2)637, 542+ (3)637, 542+ (4)637, 542+ (5)637, 542+ (6)637, 542+ (7)637, 542+ (8)637, 542+ (9)637, 542+ (10)637.

ESERCIZIO 1.2. Sia U(n) il gruppo degli elementi invertibili dell'anello $\mathbf{Z}_n$. Dati i gruppi: U(7), U(14), U(15), U(18), determinare:

a) quali sono isomorfi tra loro definendo esplicitamente un isomorfismo,
b) quali sono quelli isomorfi al gruppo $(\mathbf{Z}_6,+)$ motivando la risposta.

Sol. Il gruppo U(n) degli elementi invertibili dell'anello $\mathbf{Z}_n$ delle classi resto modulo n è costituito da tutti gli interi primi con n e minori di n. Pertanto si ha:

$$U(7) = \{1,2,3,4,5,6\}; \qquad U(14) = \{1,3,5,9,11,13\};$$
$$U(15) = \{1,2,4,7,8,11,13\}; \qquad U(18) = \{1,5,7,11,13,17\}.$$

Il Gruppo U(15) avendo sette elementi non è isomorfo ad alcuno dei rimanenti gruppi, avendo questi ultimi tutti cardinalità sei. I gruppi U(7), U(14) e U(18) sono ciclici in quanto

$$\langle 3\rangle = U(7), \ \langle 5\rangle = U(14), \ \langle 5\rangle = U(18)$$

e quindi tutti isomorfi al gruppo ciclico $(\mathbf{Z}_6,+)$. Un isomorfismo $f : G \to G'$ dal gruppo ciclico $G = \langle a\rangle$ nel gruppo ciclico $G' = \langle b\rangle$ ($|G| = |G'|$) è definito da: $f(a^n) = b^n$.

Parte II

ESERCIZIO 2.1. Si consideri lo spazio vettoriale $\mathbf{R}_3[x]$ dei polinomi a coefficienti reali di grado ≤ 3. Sia

$$W = \{(a+bx+cx^2+dx^3 \in \mathbf{R}_3[x] \ : a+d = 0 \text{ e } a-b+2c = 0\}.$$

a) Dimostrare che W è un sottospazio.
b) Determinare una base di W e quindi la sua dimensione.
c) Determinare un sottospazio U tale che $W+U = \mathbf{R}_3[x]$ e $W \cap U = \{\underline{0}\}$.
d) Il suddetto sottospazio U è unico?

Sol. (W,+) è un sottogruppo, infatti se $(a+bx+cx^2+dx^3)$, $(e+fx+gx^2+hx^3)$ sono in W si ha:

$$(a+bx+cx^2+dx^3)-(e+fx+gx^2+hx^3) = (a-e)+(b-f)x+(c-g)x^2+(d-h)x^3 \in W$$

con $(a-e)+(d-h) = (a+d)-(e+h) = 0$ e $=(a-e)-(b-f)+2(c-g) = (a-b+2c)-(e-f+2g) = 0$;
Inoltre W è chiuso rispetto alla moltiplicazione per scalari, infatti:
se $r \in \mathbf{R}$, allora $r(a+bx+cx^2+dx^3) = (ra+rbx+rcx^2+rdx^3) \in W$ e $(ra+rc) = 0$ e $(ra-rb+2rd) = 0$. Dunque W è un sottospazio.
La dimensione di W è 2 in quanto W è isomorfo a $\mathbf{R}^2$: un isomorfismo $L: \mathbf{R}^2 \to W$ è definito da: $L(c,d) = (-d+(-d+2c)x+cx^2+dx^3)$. Pertanto l'insieme ordinato:

$$B = \{1+x-x^3; 2x+x^2\}$$

è una base di W perché immagine tramite L della base canonica di $\mathbf{R}^2$.
Per determinare un sottospazio U avente somma diretta con W basta estendere B ad una base di $\mathbf{R}_3[x]$, ad esempio aggiungendo a B i vettori x^2 e x^3. L'insieme ottenuto è una base poiché le coordinate dei 4 vettori rispetto alla base canonica $\{1,x,x^2,x^3\}$

costituiscono le righe di una matrice a scala di rango 4:

$$\begin{pmatrix} 1 & 1 & 0 & -1 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Pertanto U = $<x^2; x^3>$. Un altro sottospazio avente somma diretta con W è ad esempio $<x^2; 1+x>$. Infatti la matrice

$$\begin{pmatrix} 1 & 1 & 0 & -1 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

ha rango 4.

ESERCIZIO 2.2. Sia L : $\mathbf{R^3} \to \mathbf{R}^3$ l'endomorfismo di $\mathbf{R}^3$ definito da:

$$L(1,0,0) = (1,-2,-2);\ L(1,1,0) = (1,3,-2);\ L(0,0,1) = (0,0,5).$$

Determinare:
a) la matrice A associata ad L rispetto alla base canonica,
b) gli autovalori di L e una base per ogni autospazio.
Verificare infine se L possa essere rappresentata da una matrice diagonale D ed in tal caso trovare una matrice P tale che $A = P^{-1}DP$.

Sol. La matrice A associata ad L rispetto alla base canonica ha per colonne le coordinate, rispetto alla base canonica, dei vettori L(1,0,0), L(0,1,0), L(0,0,1). Si ha: L(1,0,0) = (1,-2,-2); L(0,1,0) = L(1,1,0) - L(1,0,0) = (0,5,0); L(0,0,1) = (0,0,5) e quindi:

$$A = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 5 & 0 \\ -2 & 0 & 5 \end{pmatrix}$$

Gli autovalori di L sono gli zeri del polinomio caratteristico:

$$\det(A-\lambda I) = (1-\lambda)\,(5-\lambda)^2$$

Dunque L ha due autovalori distinti: 1 e 5 e si ha $m_a(1) = 1$ e $m_a(5) = 2$.
L'autospazio E(1) è costituito dall'insieme delle soluzioni del sistema omogeneo: $(A-I)\,X = 0$, e dunque si ha :

$$(A-I) = \begin{pmatrix} 1-1 & 0 & 0 \\ -2 & 5-1 & 0 \\ -2 & 0 & 5-1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ -2 & 4 & 0 \\ -2 & 0 & 4 \end{pmatrix} \sim_R \begin{pmatrix} -2 & 4 & 0 \\ 0 & 4 & -4 \\ 0 & 0 & 0 \end{pmatrix} \sim_R$$

$\sim_R \begin{pmatrix} -1 & 2 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix}$. Pertanto il sistema ((A−I)X = 0 è equivalente al sistema:

$$\begin{cases} -x + 2y = 0 \\ y - z = 0 \end{cases}$$

il cui insieme delle soluzioni è dato da:

$$E(1) = \{(x,y,z) \in \mathbf{R}^3 : x = 2z,\ y = z\}$$

e si ha: $m_g(1) = \dim E(1) = 1$. Una base di E(1) è {(2,1,1)}.

Poiché L(1,0,0) = 5(1,0,0) e L(0,0,1) = 5(0,0,1) e $m_g(5) \leq m_a(5) = 2$, una base di E(5) è {(0,1,0); (0,0,1)}. Infatti l'autospazio E(5) è costituito dall'insieme delle soluzioni del sistema omogeneo: (A−5I) X= 0 e quindi si ha:

$$(A-5I) = \begin{pmatrix} 1-5 & 0 & 0 \\ -2 & 5-5 & 0 \\ -2 & 0 & 5-5 \end{pmatrix} = \begin{pmatrix} -4 & 0 & 0 \\ -2 & 0 & 0 \\ -2 & 0 & 0 \end{pmatrix} \sim_R \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Pertanto il sistema ((A−5I)X = 0 è equivalente al sistema:

$$\{x = 0$$

il cui insieme delle soluzioni è dato da:

$$E(5) = \{(x,y,z) \in \mathbf{R}^3 : x = 0\},$$

e si ha $m_g(5) = \dim E(5) = 2$.

L'endomorfismo dato è dunque diagonalizzabile in quanto è definito su uno spazio vettoriale di dimensione 3 e risulta $m_g(1) + m_g(5) = 3$. La matrice diagonale

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 5 \end{pmatrix}$$

rappresenta L rispetto alla base di autovettori: {(2,1,1); (0,1,0); (0,0,1)}.

La matrice P, tale che $A = P^{-1}DP$, è l'inversa della matrice P^{-1}, quest'ultima matrice rappresenta l'identità rispetto alla base di autovettori B_a ={(2,1,1); (0,1,0); (0,0,1)} e alla base canonica, dunque le colonne di P^{-1} sono le coordinate degli autovettori di B_a rispetto alla base canonica, ossia:

$$P^{-1} = \begin{pmatrix} 2 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

Pertanto:

$$P = \frac{1}{\det(P)}\ \mathrm{Agg}(P^{-1}) = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 \\ -1 & 2 & 0 \\ -1 & 0 & 2 \end{pmatrix}.$$