CORSO di ALGEBRA (M-Z)

SCHEDA 4

(7-11-2011)

1. Anelli: l'anello K[x] dei polinomi nell'indeterminata x a coefficienti nel campo K.

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

1.2. 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 $c \in \mathbf{K}$ si dice radice del polinomio $f(x)$ se risulta $f(c) = 0$.

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

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

1.5. Posto $\mathbf{K} = \mathbf{Z}_7$. determinare le radici dei polinomi : $x^2 -1$, $x^2-3x +2$, $2x^2-x+1$. Questi polinomi sono divisibili per $(x-1)$?

1.6. In $\mathbf{Z}_{11}[x]$ 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 $f(x)g(x)$.

1.7. Posto $\mathbf{K} = \mathbf{Z}_p$ 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.

1.8. Posto $\mathbf{K} = \mathbf{Z}_5$, determinare i valori di a affinchè il polinomio (x^4+ax+a) abbia radici.

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

1.10. Sia $\mathbf{K}$ un campo. Si indichi con $\mathbf{K}(x)$ l'insieme delle endofunzioni polinomiali di $\mathbf{K}$, ossia:

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

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

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

2. Algoritmo di Euclide, MCD(a,b) e classi resto modulo n.

2.1. 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

2.2. Verificare che MCD(a,b) = MCD(a,b+ax) per ogni intero x.
2.3. Dimostrare per induzione il teorema fondamentale dell'aritmetica: ogni numero naturale $n \geq 2$ si esprime come prodotto di numeri primi.
2.4. 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.
2.5. Siano m e n interi maggiori di 1 e sia

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

pertanto:

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

Completare le seguenti frasi:

1. m divide n se.....
2. Il massimo comun divisore di m ed n è.....
3. Il minimo comune multiplo di m ed n è....
4. m/n è un intero se ....
5. m/n è un intero divisibile per p_i se ...

2.6. Dimostrare che:

1. Se MCD(a,b) = 1 allora mcm(a,b) = ab.
2. mcm(ka,kb) = k mcm(a,b).
3. Se d =MCD(a,b) allora MCD(a/d, b/d) =1.
4. mcm(a,b) = ab /MCD(a,b)

2.7. Verificare la compatibilità delle seguenti congruenze e quando possibile determinare le soluzioni:
$12x \equiv 7 \bmod 21$, $12x \equiv 7 \bmod 84$, $12x \equiv 7 \bmod 73$, $12x \equiv 7 \bmod 46$, $12x \equiv 7 \bmod 35$.
2.8. Determinare gli elementi invertibili e i rispettivi inversi di $\mathbf{Z}_6$,$\mathbf{Z}_8$,$\mathbf{Z}_{10}$ $\mathbf{Z}_{11}$.
2.9. 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?
2.10. Sia a un numero espresso in base 10 da: $a = a_n 10^n + a_{n-1} 10^{n-1} + ... a_1 10 + a_0$. Dimostrare i criteri di divisibilità:
9 divide a se e solo se 9 divide la somma delle cifre $a_n + a_{n-1} + ... a_1 + a_0$.
3 divide a se e solo se 3 divide la somma delle cifre $a_n + a_{n-1} + ... a_1 + a_0$.
5 divide a se e solo se 5 divide a_0.
11 divide a se e solo se 11 divide $a_0 - a_1 + a_2 - ... + (-1)^n a_n$
2.11. Dimostrare usando il teorema fondamentale dell'aritmetica che se p è un numero primo allora $\sqrt{p}$ è un numero irrazionale.
2.12. Dimostrare che $n(n+1)(2n+1) \equiv 0 \bmod 6$.
2.13. 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 ($\mathbf{Z}_4$,+) ?