Prova scritta di Algebra

23 giugno 2016

1. Sia $\omega = \cos(\frac{2\pi}{12}) + i\sin(\frac{2\pi}{12}) \in \mathbb{C}$ e sia $\phi : \mathbb{Z} \longrightarrow \mathbb{C}^*$ la mappa definita da $x \mapsto \omega^{7x}$.

a) Si verifichi che ϕ è un omomorfismo del gruppo $(\mathbb{Z}, +, 0)$ nel gruppo $(\mathbb{C} \setminus \{0\}, \cdot, 1)$.

b) Si determini il nucleo di ϕ.

c) Si dica se ϕ è suriettiva e si determini la controimmagine di $-\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

2. Sia G un gruppo e N un sottogruppo di G. Sia

$$Z(N) = \{a \in N \mid na = an \text{ per ogni } n \in N\}.$$

a) Si provi che $Z(N)$ è un sottogruppo normale di N.

b) Si provi che se N è normale in G, allora $Z(N)$ è un sottogruppo normale di G.

3. Siano A e B due anelli e sia $f : A \to B$ un omomorfismo suriettivo di anelli.

a) Provare che se $u \in U(A)$ allora $f(u) \in U(B)$.

b) Si consideri $A = \mathbb{Z}$, $B = \mathbb{Z}/15\mathbb{Z}$ e $f : \mathbb{Z} \to \mathbb{Z}/15\mathbb{Z}$, $f(z) = z + 15\mathbb{Z}$. Si trovi un elemento $u \in A$ non invertibile tale che $f(u)$ è invertibile in B.

4. Sia $f(x) = x^5 + x^3 + 16x^2 + 16 \in \mathbb{R}[x]$.

a) Si determinino gli ideali massimali di $\mathbb{R}[x]$ che contengono $(f(x))$.

b) Sia $g(x) = x^2 + 3 \in \mathbb{Q}[x]$ e sia $I = (g(x))$. Si dica se l'anello $\mathbb{Q}[x]/I$ contiene divisori propri dello zero motivando la risposta.

c) Con le notazioni del punto *b)*, si dica se l'elemento $x - 1 + I$ è invertibile in $\mathbb{Q}[x]/I$ e se ne determini l'inverso.

5. Determinare per quali valori del parametro $a \in \mathbb{Z}/7\mathbb{Z}$ il polinomio $p(x) = x^3 + 3x^2 + 2x + a$ è irriducibile in $\mathbb{Z}/7\mathbb{Z}[x]$. Per tali valori di a, si determini un massimo comun divisore tra $p(x)$ e $q(x) = x^2 + 5$.

Soluzioni

Esercizio 1.

a) Per ogni $x, y \in \mathbb{Z}$ si ha

$$\phi(x+y) = \omega^{7(x+y)} = \omega^{7x+7y} = \omega^{7x} \cdot \omega^{7y} = \phi(x)\phi(y).$$

Quindi ϕ è un omomorfismo di $(\mathbb{Z}, +, 0)$ in $(\mathbb{C} \setminus \{0\}, \cdot, 1)$.

b) Per definizione di nucleo di un omomorfismo si ha

$$\begin{aligned} \ker \phi &= \{z \in \mathbb{Z} \mid \phi(z) = 1\} \\ &= \{z \in \mathbb{Z} \mid \omega^{7z} = 1\} \end{aligned}$$

Osserviamo che $\omega = \cos(\frac{2\pi}{12}) + i \sin(\frac{\pi}{12})$ è un elemento del gruppo $(\mathbb{C} \setminus \{0\}, \cdot, 1)$ di periodo 12. Pertanto, per una delle proprietà del periodo degli elementi vista a lezione, si ha che $\omega^{7z} = 1$ se e solo se 12 divide $7z$ o equivalentemente $7z \equiv 0 \bmod 12$. Risolvendo la congruenza si ottiene come soluzione $z = 0 + 12k$, $k \in \mathbb{Z}$. Quindi

$$\ker \phi = 12\mathbb{Z}.$$

1. ϕ non è suriettiva perchè ad esempio non esiste nessun numero intero z tale che $\phi(z) = 2$: infatti $\phi(z) = \omega^{7z}$ è un numero complesso di norma 1, per ogni $z \in \mathbb{Z}$, mentre 2 ha norma 4.

Osserviamo che $-\frac{1}{2} + i\frac{\sqrt{3}}{2} = \omega^4$. Quindi la controimmagine di $-\frac{1}{2} + i\frac{\sqrt{3}}{2}$ è

$$\begin{aligned} \phi^{-1}(-\frac{1}{2} + i\frac{\sqrt{3}}{2}) &= \{z \in \mathbb{Z} \mid \phi(z) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}\} \\ &= \{z \in \mathbb{Z} \mid \omega^{7z} = \omega^4\} \\ &= \{z \in \mathbb{Z} \mid 7z \equiv 4 \bmod 12\} \\ &= \{z \in \mathbb{Z} \mid z = 4 + 12k, k \in \mathbb{Z}\}. \end{aligned}$$

Esercizio 2.

a) Verifichiamo prima di tutto che $Z(N)$ è un sottogruppo di N. È chiaro che $1_G \in Z(N)$. Siano $g, h \in Z(N)$ e mostriamo che $gh \in Z(N)$ e $g^{-1} \in N$. Per ogni $n \in N$ abbiamo:

$$(gh)n = g(hn) = g(nh) = (gn)h = (ng)h = n(gh)$$

quindi $gh \in Z(N)$. Inoltre per definizione, poichè $g \in Z(N)$ abbiamo che per ogni $n \in N$, $gn = ng$. Moltiplichiamo questa uguaglianza per g^{-1} a destra e a sinistra:

$$g^{-1}(gn)g^{-1} = g^{-1}(ng)g^{-1}$$

da cui

$$(g^{-1}g)ng^{-1} = g^{-1}n(gg^{-1}) \text{ e quindi } ng^{-1} = g^{-1}n.$$

Pertanto $g^{-1} \in Z(N)$.

Vediamo ora che $Z(N)$ è un sottogruppo normale di N. Questo è vero perchè, per ogni $n \in N$ e $z \in Z(N)$, abbiamo che

$$n^{-1}zn = n^{-1}nz = z \in Z(N).$$

b) Vediamo che se N è normale in G, allora $Z(N)$ è normale in G. Siano $z \in Z(N)$ e $g \in G$. Dobbiamo mostrare che $g^{-1}zg \in Z(N)$, cioè che per ogni $n \in N$ si ha

$$(g^{-1}zg)n = n(g^{-1}zg).$$

Abbiamo che

$$\begin{array}{rcll} (g^{-1}zg)n & = & (g^{-1}zg)n1_G & \text{moltiplichiamo a destra } 1_G \\ & = & (g^{-1}zg)n(g^{-1}g) & \text{scriviamo } 1_G = g^{-1}g \\ & = & g^{-1}z(gng^{-1})g & \text{per la proprietà associativa} \\ & = & g^{-1}(gng^{-1})zg & \text{perchè } gng^{-1} \in N \text{ e quindi commuta con } z \\ & = & (g^{-1}g)ng^{-1}zg & \text{per la proprietà associativa} \\ & = & n(g^{-1}zg) & \text{perchè} g^{-1}g = 1_G. \end{array}$$

Esercizio 3.

a) Supponiamo che $u \in A$ sia invertibile. Allora esiste $v \in A$ tale che $uv = 1_A = vu$. Applico f:

$$1_B = f(1_A) = f(uv) = f(u)f(v) \text{ e } 1_B = f(1_A) = f(vu) = f(v)f(u).$$

Allora $f(u)$ è invertibile in B con inverso $f(v)$.

b) Consideriamo $A = \mathbb{Z}$ e $B = \mathbb{Z}/15\mathbb{Z}$. Abbiamo che

$$U(\mathbb{Z}) = \{+1, -1\} \quad \text{e} \quad U\left(\frac{\mathbb{Z}}{15\mathbb{Z}}\right) = \{z + 15\mathbb{Z} \mid MCD(z, 15) = 1\}.$$

Quindi tutti gli elmenti $u \in \mathbb{Z}$ tali che $u \neq \pm 1$ e $MCD(u, 15) = 1$ non sono invertibili in $\mathbb{Z}$ ma $f(u) = u + 15\mathbb{Z}$ è invertibile in B. Ad esempio, $u = 2$.

Esercizio 4.

a) Gli ideali massimali di $\mathbb{R}[x]$ che contengono $(f(x))$ sono tutti e soli del tipo $(g(x))$ con $g(x)$ polinomio irriducibile che divide $f(x)$. Fattorizziamo $f(x)$ in prodotto di irriducibili in $\mathbb{R}[x]$:

$$f(x) = x^3(x^2+1)+16(x^2+1) = (x^2+1)(x^3+16) = (x^2+1)(x+2\sqrt[3]{2})(x^2-2\sqrt[3]{2}x+4\sqrt[3]{4}).$$

Pertanto gli ideali massimali di $\mathbb{R}[x]$ che contengono $(f(x))$ sono $(x^2 + 1)$, $(x + 2\sqrt[3]{2})$ e $(x^2 - 2\sqrt[3]{2}x + 4\sqrt[3]{4})$.

b) $g(x)$ è irriducibile in $\mathbb{Q}[x]$ per il criterio di Eisenstein (con $p = 3$) e quindi l'anello $\mathbb{Q}[x]/I$ è un campo. In particolare non contiene divisori propri di zero, perchè gli elementi invertibili non possono essere divisori di zero.

c) L'elemento $x-1+I$ è invertibile in $\mathbb{Q}[x]/I$ perchè è un elemento diverso da zero di un campo. Determino l'inverso.

$$\begin{array}{rr|l} x^2 & +3 & x-1 \\ \cline{3-3} -x^2+x & & x+1 \\ \cline{1-2} x & +3 & \\ -x & +1 & \\ \cline{1-2} & 4 & \end{array}$$

Quindi

$$4 = (x^2 + 3) - (x - 1)(x + 1)$$

$$1 = \frac{1}{4}(x^2 + 3) + (x - 1)(-\frac{1}{4}x - \frac{1}{4})$$

e l'inverso di $x - 1 + I$ è $(-\frac{1}{4}x - \frac{1}{4}) + I$.

Esercizio 5. Essendo di grado 3, $p(x)$ è irriducibile in $\mathbb{Z}/7\mathbb{Z}[x]$ se e solo se non ha radici in $\mathbb{Z}/7\mathbb{Z}$. Cerco le radici:

$$p(0) = a,\ p(1) = 6 + a,\ p(2) = 3 + a,\ p(3) = 4 + a,$$

$$p(4) = p(-3) = 1 + a,\ p(5) = p(-2) = a,\ p(6) = p(-1) = a.$$

Quindi il polinomio ha radici per i valori di a che annullano tutte le quantità calcolate, cioè $a \in \{0, 1, 3, 4, 6\}$ mentre è irriducibile per $a \in \{2, 5\}$.

Supponiamo ora che $a \in \{2, 5\}$. Allora $p(x)$ è irriducibile e quindi il massimo comun divisore tra $p(x)$ e $x^2 + 5$, essendo un divisore di $p(x)$, può essere solo $p(x)$ oppure 1. Notiamo che $p(x)$ non divide $x^2 + 5$ (per ragioni di ordine) e quindi il massimo comun divisore è 1 (o un altro elemento non nullo di $\mathbb{Z}/7\mathbb{Z}$).