Algebra 1

Prof. E. Spinelli

Secondo Esonero

7 Giugno 2016

Nome e Cognome: ____________________

Numero di Matricola: ____________________

Esercizio	Punti totali	Punteggio
1	6	
2	6	
3	6	
4	6	
5	6	
Totale	30	

ATTENZIONE:
- I COMPITI DISORDINATI O POCO LEGGIBILI NON SARANNO NEANCHE CORRETTI
- **GIUSTIFICATE LE VOSTRE ARGOMENTAZIONI**
- SCRIVETE LE RISPOSTE NEGLI APPOSITI RIQUADRI
- I FOGLI DI BRUTTA NON SARANNO ACCETTATI
- TUTTI I DISPOSITIVI ELETTRONICI (CALCOLATRICI, SMARTPHONES, TABLETS, TELEFONINI ETC ...) DEVONO ESSERE SPENTI E IN BORSA
- NON SONO AMMESSI LIBRI O APPUNTI.

Esercizio 1. Sia A un anello commutativo unitario e $d \in A$ tale che $d^2 = d$. Poniamo $A_d := \{x \,|\, x \in A, \quad xd = 0_A\}$.

(a) Provare che A_d è un ideale di A.

(b) Determinare un ideale I di A ed un isomorfismo $f : A/A_d \longrightarrow I$.

(c) Dire se i precedenti asserti valgono nel caso in cui $d^2 \neq d$.

Soluzione: (a) e (b) Sia $I := (d)_A = \{ad \,|\, a \in A\}$ l'ideale generato da d in A e consideriamo l'applicazione

$$g : A \longrightarrow I, \qquad a \longmapsto ad.$$

Verifichiamo che g è un omomorfismo. A tal fine, siano $a, b \in A$. Allora

$$g(a + b) = (a + b)d = ad + bd = g(a) + g(b)$$

e

$$g(ab) = (ab)d = (ab)d^2 = (ad)(bd) = g(a)g(b)$$

sfruttando l'ipotesi su d ed il fatto che A sia commutativo.

Inoltre, se $x \in A$

$$x \in \text{Ker } g \iff g(x) = 0_A \iff xd = 0_A \iff x \in A_d.$$

Pertanto $A_d = \text{Ker } g$ e quindi è un ideale di A.

Per il Teorema di omomorfismo per anelli $A/\text{Ker } g \cong A/A_d \cong g(A) = I$, essendo g suriettivo. Quindi l'applicazione f cercata è tale che

$$f(a + A_d) = ad \qquad \forall\, a \in A.$$

(c) Si sfrutta il fatto che $d^2 = d$ per verificare che g, e quindi f, è un omomorfismo.

Verifichiamo che in ogni caso I è un ideale di A. Infatti $0_A \in A_d$, quindi $A_d \neq \emptyset$. Siano ora $x, y \in A_d$. Allora

$$(x - y)d = xd - yd = 0_A - 0_A = 0_A,$$

ovvero $x - y \in A_d$ e pertanto $(A_d, +) \leq (A, +)$. Infine, se $a \in A$

$$(xa)d = (ax)d = a(xd) = a0_A = 0_A,$$

e questo prova quanto asserito.

Risposta:

(b) $f(a + A_d)=$ $\boxed{ad}$ (c) Vale (a) $\boxed{\text{SI}}$ (c) Vale (b) $\boxed{\text{NO}}$

Esercizio 2. Sia G un gruppo e $Z(G) := \{x \mid x \in G, \quad xy = yx \ \ \forall y \in G\}$ il centro di G (che sappiamo essere un sottogruppo normale di G). Se $G/Z(G)$ è ciclico, e $xZ(G)$ è un suo generatore, provare che G è abeliano.

Soluzione: G è unione delle classi laterali destre di $Z(G)$ in G un cui sistema di rappresentanti, essendo $G/Z(G) = \langle xZ(G) \rangle$, è dato dalle potenze di x. Quindi, se $a, b \in G$ esistono $m, n \in \mathbb{Z}$ e $h, k \in Z(G)$ tali che $a = x^m h$ e $b = x^n k$. Pertanto

$$ab = x^m h x^n k = x^{m+n} hk = x^{m+n} kh = x^n k x^m h = ba.$$

Per l'arbitrarietà di a e b si ha che G è abeliano.

Esercizio 3. Sia $\mathbb{Z}_5 := \mathbb{Z}/\equiv_5$, $f := x^2 + ax + 3 \in \mathbb{Z}_5[x]$ e $I := (f)_{\mathbb{Z}_5[x]}$.

(a) Determinare per quali valori di a l'anello $\mathbb{Z}_5[x]/I$ ha divisori dello zero.

(b) Per ogni a determinare gli ideali massimali di $\mathbb{Z}_5[x]/I$.

Soluzione: (a) L'anello $\mathbb{Z}_5[x]/I$ ha divisori dello zero se non è un dominio (quindi un campo, essendo finito). Pertanto I deve essere generato da un polinomio non irriducibile il che, essendo f di grado 2, si riduce a determinare i valori di a per cui f ammette radici. Facili calcoli stabiliscono che tali valori sono 1 e 4.

(b) Per $a \notin \{1, 4\}$ si ha che $\mathbb{Z}_5[x]/I$ è un campo ed ha un unico ideale massimale $\{0_{\mathbb{Z}_5[x]/I}\}$.

Per $a = 1$ risulta $f = (x + 2)(x + 4)$. Per il Teorema di corrispondenza degli ideali di un anello quoziente, posto $K := (x + 2)_{\mathbb{Z}_5[x]}$ e $H := (x + 4)_{\mathbb{Z}_5[x]}$ gli ideali di $\mathbb{Z}_5[x]/I$ sono, oltre a quelli banali,

$$H/I \qquad \text{e} \qquad K/I$$

che sono anche gli unici massimali.

Per $a = 4$ si ha che $f = (x + 1)(x + 3)$ e, ragionando come sopra, si conclude che gli unici ideali massimali di $\mathbb{Z}_5[x]/I$ sono

$$L/I \qquad \text{e} \qquad M/I,$$

dove $L := (x + 1)_{\mathbb{Z}_5[x]}$ e $M := (x + 3)_{\mathbb{Z}_5[x]}$.

Risposta: (a) $a = \boxed{1, 4}$

Esercizio 4. Dati i gruppi $(\mathbb{Z}, +)$ e $(\mathcal{S}_5, \circ)$ (il gruppo simmetrico su 5 elementi) determinare per quali valori di n esiste un omomorfismo di gruppi $f : \mathbb{Z} \longrightarrow \mathcal{S}_5$ tale che $|f(\mathbb{Z})| = n$.

Soluzione: Sia f un omomorfismo da $(\mathbb{Z}, +)$ in $(\mathcal{S}_5, \circ)$. Allora, per il Teorema di omomorfismo, $\mathbb{Z}/\mathrm{Ker}\, f \cong f(\mathbb{Z})$. In particolare, essendo i quozienti di $\mathbb{Z}$ gruppi ciclici, $f(\mathbb{Z})$ deve essere un gruppo ciclico. Pertanto $|f(\mathbb{Z})| = \mathrm{o}(\alpha)$ per un opportuno $\alpha \in \mathcal{S}_5$.

Ora, per $2 \leq m \leq 5$, i cicli di lunghezza m in $\mathcal{S}_5$ hanno ordine m. Inoltre ogni permutazione non identica è prodotto di cicli disgiunti. Quindi se un sottogruppo ciclico non-banale di $\mathcal{S}_5$ non è generato da un ciclo o da un prodotto di due trasposizioni disgiunte (che ha ordine 2) deve essere prodotto di una trasposizione e di un ciclo di lunghezza 3 e tale permutazione ha ordine $\mathrm{mcm}(2, 3) = 6$. Inoltre $\mathrm{id}_{\mathcal{S}_5}$ genera un sottogruppo con un solo elemento. Quindi $|f(\mathbb{Z})| \in \{1, \ldots, 6\}$.

Infine, sia $\alpha \in \mathcal{S}_5$ di ordine n (quindi minore o uguale a 6). L'applicazione $f : \mathbb{Z} \longrightarrow \mathcal{S}_5$ tale che

$$f(0) = \mathrm{id}_{\mathcal{S}_5}, \qquad f(1) = \alpha \qquad \text{e} \qquad f(t) = \alpha^t$$

per ogni $t \in \mathbb{Z}$ definisce effettivamente un omomorfismo da $(\mathbb{Z}, +)$ in $(\mathcal{S}_5, \circ)$ tale che $|f(\mathbb{Z})| = n$.

Risposta:

$n = \boxed{1, 2, 3, 4, 5, 6}$

Esercizio 5. Si consideri il sottoinsieme di $\mathbb{Z}[i]$, $I := \{a \,|\, a \in \mathbb{Z}[i], \quad ||a|| \equiv_2 0\}$.

(a) Provare che I è un ideale di $\mathbb{Z}[i]$.

(b) Dire se I è primo.

(c) Determinare $|\mathbb{Z}[i]/I|$.

Soluzione: Consideriamo la funzione

$$g : \mathbb{Z}[i] \longrightarrow \mathbb{Z}/\equiv_2, \qquad a \longmapsto [||a||]_{\equiv_2}.$$

Verifichiamo che g è un omomorfismo. A tal fine, siano $a + ib, c + id \in \mathbb{Z}[i]$. Allora

$$\begin{aligned} g((a+ib)+(c+id)) = g((a+c)+i(b+d)) &= [a^2+c^2+2ac+b^2+d^2+2bd]_{\equiv_2} = [a^2+c^2+b^2+d^2]_{\equiv_2} \\ &= [a^2+b^2]_{\equiv_2} \hat{+} [c^2+d^2]_{\equiv_2} = g(a+ib) \hat{+} g(c+id) \end{aligned}$$

e

$$g((a+ib)(c+id)) = [||(a+ib)(c+id)||]_{\equiv_2} = [||a+ib||]_{\equiv_2} \hat{\cdot} [||c+id||]_{\equiv_2} = g(a+ib) \hat{\cdot} g(c+id).$$

Banalmente g è suriettivo ($g(0) = [0]_{\equiv_2}$ e $g(1) = [1]_{\equiv_2}$).

Ora, se $\alpha \in Z[i]$

$$\alpha \in \text{Ker } g \iff [||\alpha||]_{\equiv_2} = [0]_{\equiv_2} \iff \alpha \in I.$$

Pertanto $I = \text{Ker } g$ e quindi è un ideale di $\mathbb{Z}[i]$. Inoltre per il Teorema di omomorfismo per anelli $\mathbb{Z}[i]/I \cong \mathbb{Z}/\equiv_2$ che è un campo e dunque I è primo e $|\mathbb{Z}[i]/I| = 2$.

(b) I è primo $\boxed{\text{SI}}$ (c) $|\mathbb{Z}[i]/I| = \boxed{2}$