Algebra 1

Proff. P. Piazza, E. Spinelli

Primo Esame

1 Luglio 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.

Orale:

I Luglio ☐ II Luglio ☐ I Settembre ☐ II Settembre ☐

Esercizio 1. Determinare per quali valori di a e b il seguente sistema ha soluzioni (*non è richiesto di determinarle*)

$$\begin{cases} aX \equiv 8 \mod 14 \\ X \equiv 2b \mod 6 \end{cases}$$

Soluzione: Affinchè il sistema sia compatibile deve verificarsi che almeno entrambe le equazioni che lo compongono abbiano soluzione. Ora la seconda equazione ha soluzione per ogni $b \in \mathbb{Z}$ in quanto $\mathrm{mcd}(1,6) = 1$ divide $2b$. La prima equazione ha invece soluzione quando $\mathrm{mcd}(a,14)$ divide 8, ovvero $\mathrm{mcd}(a,14) \in \{1,2\}$.

Se $\mathrm{mcd}(a,14) = 2$, posto $a' := \frac{a}{2}$, il sistema è equivalente a

$$\begin{cases} a'X \equiv 4 \mod 7 \\ X \equiv 2b \mod 6 \end{cases}$$

che è facilmente riconducibile ad uno del tipo cinese dei resti (osserviamo che $\mathrm{mcd}(a',7) = 1$).

Se $\mathrm{mcd}(a,14) = 1$, consideriamo l'equzione

$$a(2b + 6h) \equiv_{14} 8$$

nell'incognita h (si sta imponendo che una generica soluzione della seconda equazione del sistema sia una soluzione della prima). Vale che

$$a(2b + 6h) \equiv_{14} 8 \quad \iff \quad a(b + 3h) \equiv_7 4 \quad \iff \quad 3ah \equiv_7 4 - ab,$$

che ha chiaramente soluzione in quanto $\mathrm{mcd}(3a,7) = 1$.

Pertanto il sistema ha soluzione per ogni valore di a tale che $\mathrm{mcd}(a,14) \in \{1,2\}$, indipendentemente dal valore di b.

Risposta:

a è tale che $\boxed{}$ b è tale che $\boxed{}$

Esercizio 2. Sia G un gruppo e $H \leq G$. Provare che

(a) per ogni $g \in G$ l'insieme $H^g := \{g^{-1}hg \,|\, h \in H\}$ è un sottogruppo di G isomorfo a H;

(b) se G è finito e $H \trianglelefteq G$, H ciclico, allora per ogni K sottogruppo di H si ha che $K \trianglelefteq G$ (*utilizzare il punto (a) e le proprietà dei sottogruppi di un gruppo ciclico finito*).

Soluzione: (a) Sia $g \in G$. L'insieme H^g è non vuoto poichè $1_G^g = 1_G \in H^g$.
Siano ora $h_1^g, h_2^g \in H^g$. Allora

$$(h_1^g)(h_2^g)^{-1} = g^{-1}h_1g(g^{-1}h_2g)^{-1} = g^{-1}h_1gg^{-1}h_2^{-1}g = g^{-1}h_1h_2^{-1}g = (h_1h_2^{-1})^g,$$

che è in H^g in quanto $h_1h_2^{-1} \in H$. Per la caratterizzazione dei sottogruppi di un gruppo si ha che $H^g \leq G$.
Consideriamo l'applicazione

$$\phi_g : H \longrightarrow H^g, \qquad h \longmapsto g^{-1}hg.$$

Banalmente ϕ_g è biettiva. Siano ora $h_1, h_2 \in H$. Si ha

$$\phi_g(h_1h_2) = g^{-1}h_1h_2g = (g^{-1}h_1g)(g^{-1}h_2g) = \phi_g(h_1)\phi_g(h_2).$$

Pertanto ϕ_g è un omomorfismo, quindi un isomorfismo di gruppi.

(b) Sia sempre $g \in G$. Per il punto (a), K^g è isomorfo a K e quindi $|K^g| = |K|$ e, poichè $K \leq H$ e $H \trianglelefteq G$, $K^g \leq H$. Per l'unicità dei sottogruppi di dato ordine di un gruppo ciclico finito si ha che $K^g = K$, ovvero che $K \trianglelefteq G$.

Esercizio 3. Sia $\mathbb{Z}_7 := \mathbb{Z}/\equiv_7$, $f := x^3 + ax^2 + 5x + 3 \in \mathbb{Z}_7[x]$ e $I := (f)_{\mathbb{Z}_7[x]}$.

(a) Determinare per quali valori di a l'anello $\mathbb{Z}_7[x]/I$ è un campo.

(b) Per $a = 5$ stabilire se $x + 2$ ha inverso in $\mathbb{Z}_7[x]/I$.

Soluzione: (a) L'anello $\mathbb{Z}_7[x]/I$ è un campo se, e solo se, l'ideale I è massimale ovvero se, e solo se, il polinomio f è irriducibile. Essendo $\mathbb{Z}_7$ un campo e f di grado 3 questo accade quando f non ha radici in $\mathbb{Z}_7$ e quindi per $a \in \{1, 4, 6\}$ (per $a = 0$, 2 è radice; per $a = 2$, 3 è radice; per $a = 3$, 6 è radice; per $a = 5$, 1 è radice).

(b) Vale che $x^3 + 5x^2 + 5x + 3 = (x + 2)(x^2 + 3x + 6) + 5$, ed essendo 5 invertibile in $\mathbb{Z}_7$ segue che $x + 2$ ha inverso in $\mathbb{Z}_7[x]/I$.

Risposta: (a) $a =$ $\square$ (b) $x + 2$ ha inverso? $\square$

Esercizio 4. Sia G un gruppo e si consideri l'insieme $G \times G$ munito del prodotto componente per componente (il prodotto diretto di G e G) che è un gruppo. Sia $D := \{(a,a) \mid a \in G\}$. Provare che

(a) $D \leq G \times G$;

(b) $D \trianglelefteq G \times G$ se, e solo se, G è abeliano;

(c) se $D \trianglelefteq G \times G$ allora $G \times G/D$ è isomorfo a G.

Soluzione: (a) L'insieme D è non vuoto poichè $(1_G, 1_G) \in D$.
Siano ora $(a,a), (b,b) \in D$. Allora

$$(a,a)(b,b)^{-1} = (a,a)(b^{-1},b^{-1}) = (ab^{-1}, ab^{-1}) \in D.$$

Per la caratterizzazione dei sottogruppi di un gruppo si ha che $D \leq G \times G$.

(b) Assumiamo che G sia abeliano e sia $(x,x) \in D$ e $(g,h) \in G \times G$. Vogliamo provare che D è normale in $G \times G$, ovvero che $(x,x)^{(g,h)} \in D$. Ma

$$(g,h)^{-1}(x,x)(g,h) = (g^{-1},h^{-1})(x,x)(g,h) = (g^{-1}xg, h^{-1}xh) = (x,x) \in D$$

per l'abelianità di G.
Viceversa, siano $x, y \in G$. Si ha che

$$(x,x)^{(1_G,y)} = (x, y^{-1}xy)$$

è un elemento di D poichè $D \trianglelefteq G \times G$. Pertanto deve essere $y^{-1}xy = x$, i.e. $xy = yx$. Per l'arbitrarietà di x e y si conclude che G è abeliano.

(c) Si consideri la funzione

$$f : G \times G \longrightarrow G, \qquad (x,y) \longmapsto xy^{-1}$$

e siano $(x,y), (z,w) \in G \times G$. Vale che

$$f((x,y)(z,w)) = f(xz, yw) = xz(yw)^{-1} = xzw^{-1}y^{-1} = (xy^{-1})(zw^{-1}) = f(x,y)f(z,w),$$

essendo G abeliano per il punto (b). Quindi f è un omomorfismo di gruppi.
Sia ora $g \in G$. Allora

$$f(g, 1_G) = g1_G^{-1} = g.$$

Pertanto f è suriettivo.
Infine, se $(x,y) \in G \times G$,

$$(x,y) \in \mathrm{Ker} f \iff f(x,y) = 1_G \iff xy^{-1} = 1_G \iff x = y \iff (x,y) \in D.$$

Per il Teorema di omomorfismo per gruppi si conclude che $G \times G/D \cong f(G \times G) = G$, che è quanto volevasi provare.

Esercizio 5. Si consideri l'ideale I di $\mathbb{Z}[i]$ generato dagli elementi $3+6i$ e $3+i$.

(a) Determinare se I è un ideale primo di $\mathbb{Z}[i]$.

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

Soluzione: (a) La decomposizione in elementi primi di $3+6i$ e $3+i$ è

$$3+6i = 3(1+2i), \qquad 3+i = (1+2i)(1-i).$$

Quindi $I = (\mathrm{mcd}(3+6i, 3+i))_{\mathbb{Z}[i]} = (1+2i)_{\mathbb{Z}[i]}$ è un ideale primo di $\mathbb{Z}[i]$ essendo il suo generatore un elemento primo di $\mathbb{Z}[i]$ (ricordiamo che $\mathbb{Z}[i]$ è dominio euclideo).

(b) Un sistema di rappresentanti per $\mathbb{Z}[i]/I$ conterrà solo elementi di norma strettamente minore di $||1+2i|| = 5$.

- 0 è l'unico elemento di norma 0;
- $\pm 1, \pm i$ sono gli unici elementi di norma 1;
- $1+i, 1-i, -1+i, -1-i$ sono gli unici elementi di norma 2;
- non ci sono elementi di norma 3;
- $\pm 2, \pm 2i$ sono gli unici elementi di norma 4.

Gli elementi di $\mathbb{Z}[i]/I$

$$I, 1+I, -1+I, -i+I, i+I$$

sono tutti distinti (altrimenti I conterrebbe elementi di norma strettamente minore di 5.

Vale inoltre che

$$(1+i)+I = -i+I,\ (-1-i)+I = i+I,\ (1-i)+I = -1+I,\ (-1+i)+I = 1+I.$$

Infine

$$-2+I = -i+I,\ 2i+I = -1+I,\ 2+I = i+I,\ -2i+I = 1+I.$$

Pertanto $\mathbb{Z}[i]/I = \{I, 1+I, -1+I, -i+I, i+I\}$ e quindi $|\mathbb{Z}[i]/I| = 5$.

(a) I è primo $\boxed{}$ (c) $|\mathbb{Z}[i]/I| = \boxed{}$