Algebra 1

Proff. P. Piazza, E. Spinelli

Terzo Esame

9 Settembre 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 Settembre ☐ II Settembre ☐

Esercizio 1. Dimostrare che

(a) per ogni $n \in \mathbb{N}$, 4 divide $(-1)^n(2n+1)-1$;

(b) se $a, b \in \mathbb{Z}$ e $m := 10a + b$, allora 7 divide m se, e solo se, $4a \equiv_7 b$;

(c) per ogni $n \in \mathbb{N}$, 11 divide $n^{12} - n^2$.

Soluzione: (a) Procediamo per induzione su n. Per $n = 0$ l'asserto è banale.
Sia ora $n \geq 0$ e supponiamo l'asserto vero per n. Vale che

$$(-1)^{n+1}(2(n+1)+1)-1 = (-1)[(-1)^n(2n+1)-1] + (-1)^{n+1}2 - 2.$$

Ora, per l'ipotesi induttiva, 4 divide $[(-1)^n(2n+1)-1]$ e quindi anche $(-1)[(-1)^n(2n+1)-1]$. Inoltre 4 divide anche $(-1)^{n+1}2-2$, essendo tale elemento uguale a 0 o a 4, e questo conclude la dimostrazione.
(b) Vale che

$$7 \mid m \iff 10a + b \equiv_7 0 \iff -3a \equiv_7 b \iff 4a \equiv_7 b.$$

(c) Sia $n \in \mathbb{N}$. Se 11 divide n, allora divide anche $n^{12} - n^2$. Supponiamo pertanto che 11 non divida n, ossia $\mathrm{mcd}(n, 11) = 1$. Allora per Fermat $n^{10} \equiv_{11} 1$ e quindi, moltiplicando ambo i membri per n^2, $n^{12} \equiv_{11} n^2$, che è quanto volevasi provare.

Esercizio 2. Sia G un gruppo, $H \trianglelefteq G$ e $K \leq G$ tali che $G = HK := \{hk \,|\, h \in H,\ k \in K\}$. Provare che

(a) $H \cap K \trianglelefteq K$;

(b) se H è abeliano, $H \cap K \trianglelefteq G$.

Soluzione: (a) Sia $x \in H \cap K$ e $y \in K$. Allora

$$y^{-1}xy \in K$$

perchè sia x che y sono in K che è sottogruppo di G. D'altro canto tale elemento è anche in H poichè $x \in H$ (essendo in $H \cap K$) e H è normale in G. In conclusione $y^{-1}xy \in H \cap K$, ovvero $H \cap K \trianglelefteq K$.
(b) Sia $x \in H \cap K$ e $g \in K$. Poichè $G = HK$, esistono $h \in H$ e $k \in K$ tali che $g = hk$. Ora

$$g^{-1}xg = (hk)^{-1}x(hk) = k^{-1}(h^{-1}xh)k = k^{-1}xk$$

essendo x e h elementi del gruppo abeliano H. Pertanto $g^{-1}xg$ è in K, ma anche in H (sempre invocando il fatto che $x \in H \trianglelefteq G$), e quindi $H \cap K \trianglelefteq G$.

Esercizio 3. Sia G un gruppo abeliano, $n \in \mathbb{N}$ e si ponga

$$G^n := \{x^n \mid x \in G\}, \qquad G_n := \{x \mid x \in G, \quad x^n = 1_G\}.$$

Provare che

(a) G^n e G_n sono sottogruppi di G;

(b) G/G_n è isomorfo a G^n.

Soluzione: Consideriamo la funzione

$$f : G \longrightarrow G, \qquad x \longmapsto x^n.$$

Se $x, y \in G$

$$f(xy) = (xy)^n = x^n y^n = f(x)f(y)$$

sfruttando l'abelianità di G. Pertanto f è un endomorfismo di G la cui immagine coincide con G^n, che dunque risulta essere un sottogruppo di G.

Infine, se $x \in G$, vale

$$x \in \mathrm{Ker} f \quad \Longleftrightarrow \quad f(x) = x^n = 1_G \quad \Longleftrightarrow \quad x \in G_n.$$

Da questo segue che $G_n = \mathrm{Ker} f \leq G$ e, per il Teorema di isomorfismo per gruppi, che G/G_n è isomorfo a G^n.

Esercizio 4. Sia A un anello commutativo unitario finito. Provare che ogni $x \in A \setminus \{0_A\}$ che non è un divisore dello zero è invertibile (*Suggerimento: si consideri per ogni* $x \neq 0_A$ *la funzione* $f_x : A \longrightarrow A$ *tale che* $f_x(y) = xy$).

Soluzione: Per ogni $x \in A \setminus \{0_A\}$ si consideri la funzione

$$f_x : A \longrightarrow A, \qquad y \longmapsto xy.$$

Supponiamo prima che f_x non sia iniettiva. Allora esistono $a, b \in A$ con $a \neq b$ tali che

$$xa = f_x(a) = f_x(b) = xb.$$

Questo implica che $x(a - b) = 0_A$ e dunque x è un divisore dello zero essendo $a - b \neq 0_A$.

Assumiamo pertanto che f sia iniettiva ovvero, poichè A è finito, biettiva. Quindi esiste $y \in A$ tale che

$$1_A = f_x(y) = xy,$$

cioè x è un elemento invertibile di A.

Esercizio 5. Se $n \in \mathbb{N}$, si ponga $\mathbb{Z}_n := \mathbb{Z}/\equiv_n$. Determinare per quali valori di $n \in \mathbb{P}$ l'mcd$(x^2 + x + 1, x^4 + 3x^3 + x^2 + 7x + 5)$ è invertibile in $\mathbb{Z}_n[x]$.

Soluzione: Vale che

$$x^4 + 3x^3 + x^2 + 7x + 5 = (x^2 + x + 1)(x^2 + 2x - 2) + 7x + 7.$$

Ora, se $n = 7$, $7x + 7 = 0$ in $\mathbb{Z}_n[x]$ e quindi $\mathrm{mcd}(x^2 + x + 1, x^4 + 3x^3 + x^2 + 7x + 5) = x^2 + x + 1$ che non è invertibile in $\mathbb{Z}_n[x]$.

Pertanto, assumiamo che $n \neq 7$, e dunque che 7 sia invertibile in $\mathbb{Z}_n$. Allora,

$$x^2 + x + 1 = (7x + 7)(7^{-1}x) + 1,$$

da cui segue che $\mathrm{mcd}(x^2 + x + 1, x^4 + 3x^3 + x^2 + 7x + 5) = 1$.