UNIVERSITÀ DEGLI STUDI ROMA TRE
Corso di Laurea in Matematica
AL2 - Algebra 2 - Gruppi, Anelli e Campi - A.A. 2008/2009

Appello B

MATRICOLA: .....

COGNOME: ..... **NOME:** .....

Avvertenza: Svolgere ogni esercizio nello spazio assegnato, senza consegnare altri fogli e giustificando tutte le affermazioni fatte. Non è consentito l'utilizzo di libri e appunti.

ESERCIZIO 1. (4 pt) Sia G un gruppo. Dimostrare che se $G/Z(G)$ è ciclico allora G è abeliano.

ESERCIZIO 2. Sia $n \geq 3$ un numero naturale e siano:

$$H_1 := \{\sigma \in S_n : \sigma(n) = n\},$$

$$H_2 := \{\sigma \in S_n : \sigma(n) \neq 1\}.$$

(a) (2 pt) Calcolare la cardinalità di H_1 e H_2.
(b) (4 pt) Stabilire se H_1 e H_2 sono sottogruppi di S_n e se sono normali.

ESERCIZIO 3. Sia $\mathbb{M}(\mathbb{N}, \mathbb{Z}) := \{f : \mathbb{N} \to \mathbb{Z}\}$ linsieme delle funzioni da $\mathbb{N}$ in $\mathbb{Z}$ con le operazioni indotte da $\mathbb{Z}$, cioè :

$$(f + g)(n) := f(n) + g(n), \quad (fg)(n) := f(n)g(n), \ \forall \in \mathbb{N}.$$

Sappiamo che $\mathbb{M}(\mathbb{N}, \mathbb{Z})$ con le due operazioni appena descritte è un anello commutativo con unità .

(a) (4 pt) Descrivere gli insiemi dei divisori di zero e degli elementi invertibili di $\mathbb{M}(\mathbb{N}, \mathbb{Z})$ e stabilire se sono ideali di $\mathbb{M}(\mathbb{N}, \mathbb{Z})$.
(b) (2 pt) Per ogni sottoinsieme X di $\mathbb{N}$ si definisce:

$$I(X) := \{f \in \mathbb{M}(\mathbb{N}, \mathbb{Z}) \mid f(x) = 0, \ \forall x \in X\}.$$

Dimostrare che $I(X)$ è un ideale di $\mathbb{M}(\mathbb{N}, \mathbb{Z})$.
(c) (2 pt) Dimostrare che se $I(X)$ è primo allora X ha al più un elemento.
(d) (2 pt) Stabilire se $I(\{0\})$ è un ideale primo e/o massimale.

ESERCIZIO 4. Sia

$$\varphi : \mathbb{Z}[i] \to \mathbb{Z}_{13}, \quad (a + bi) := a + 5b.$$

(a) (2 pt) Mostrare che φ è un omomorfismo di anelli e stabilire se esso è iniettivo e/o suriettivo;
(b) (2 pt) Trovare un generatore per $Ker(\varphi)$;
(c) (2 pt) Applicare il Teorema di Omomorfismo per caratterizzare l'anello quoziente $\mathbb{Z}[i]/ker(\varphi)$.

ESERCIZIO 5. Sia $f_\alpha(X) = X^3 - X^2 + X + \alpha \in \mathbb{Z}_5[X]$ ed $I_\alpha := (f_\alpha(X))$.

(a) (3 pt) Determinare per quali valori di α in $\mathbb{Z}_5$ lanello quoziente $\mathbb{Z}_5[X]/I_\alpha$ è un campo.

(b) (3 pt) Stabilire se la classe $(X^5-X^4+3)+I_2$ è invertibile in $\mathbb{Z}_5[X]/I_2$ e calcolare il suo inverso.

SOLUZIONI

ESERCIZIO 1. Ogni elemento di G appartiene ad una classe laterale di $Z(G)$ (questo vale per un qualsiasi sottogruppo di G, anche diverso da $Z(G)$, in quanto le classi laterali di un sottogruppo formano una partizione del gruppo). Quindi $a \in G \Rightarrow a \in hZ(G) \Rightarrow a = hz$, con $h \in G$, $z \in Z(G)$. Poiché il quoziente $G/Z(G)$ è ciclico, tutte le classi laterali di $Z(G)$ sono del tipo $g^iZ(G)$. Dunque tutti gli elementi di G sono del tipo g^iz, con $z \in Z(G)$. Prendiamo due elementi $a, b \in G$, con $a = g^iz_1$, $b = g^jz_2$. Allora:

$$ab = g^iz_1g^jz_2 = g^ig^jz_1z_2 = g^jg^iz_2z_1 = g^jz_2g^iz_1 = ba,$$

sfruttando il fatto che gli elementi del centro commutano sempre e che $g^ig^j = g^jg^i$, per un qualsiasi elemento $g \in G$.

ESERCIZIO 2.

(a) Si vede facilmente che $\mid H_1 \mid = (n-1)!$, in quanto un elemento resta fermo e tutti gli altri $n-1$ si possono permutare fra di loro in qualsiasi modo. Per quanto riguarda H_2 invece si ha che i primi $n-1$ elementi $1, 2, \cdots n-1$ possono essere permutati fra di loro in qualsiasi modo, mentre n può variare solo fra $n-1$ elementi, quindi $\mid H_1 \mid = (n-1)\cdot(n-1)!$.

(b) Si vede subito che H_2 non può essere un sottogruppo di S_n perché $(n-1)\cdot(n-1)!$ non divide $n!$ (in quanto $n-1$ non divide n a meno che $n = 2$).

H_1 è un sottogruppo poiché se una permutazione σ fissa n anche la sua inversa fisserà n e così anche la composizione $\sigma \circ \tau^{-1}$ se σ e τ stanno in H_1.

H_1 non è normale : si vede con un controesempio. Prendiamo $\sigma = (1,2) \in H_1$ e $\tau = (1,n) \in S_n$. Allora $\tau \circ \sigma \circ \tau^{-1} = (1,n)(1,2)(1,n) = (2,n) \notin H_1$.

ESERCIZIO 3.

(a) Divisori dello zero = tutte le funzioni $f \in \mathbb{M}(\mathbb{N}, \mathbb{Z})$ che non sono identicamente nulle (cioè non sono costantamente uguali a 0) e che si annullano in almeno un punto. Infatti se $f(Y) \neq 0$, per qualche sottoinsieme $Y \subsetneq \mathbb{N}$, e $f \neq 0$, allora scegliendo $g \in \mathbb{M}(\mathbb{N}, \mathbb{Z})$ tale che $g(\mathbb{N} \backslash Y) = 0$ e $g \neq 0$, si ha che $fg = 0$ pur essendo f e g due funzioni non nulle.

Un elemento invertibile, in generale, non può mai essere un divisore dello zero, quindi questa considerazione già esclude che le funzioni viste nel paragrafo precedente possano essere invertibili. Una funzione $f \in \mathbb{M}(\mathbb{N}, \mathbb{Z})$ è invertibile se esiste $g \in \mathbb{M}(\mathbb{N}, \mathbb{Z})$ tale che $fg = 1$, cioè $f(n)g(n) = 1$, per ogni $n \in \mathbb{N}$. Poiché i valori delle funzioni considerate sono in $\mathbb{Z}$, possiamo solo avere $f(n) = g(n) = 1$ oppure $f(n) = g(n) = -1$. Quindi le funzioni invertibili sono quelle tali che $f(\mathbb{N}) = \{\pm 1\}$.
Né gli elementi invertibili né i divisori dello zero formano mai un ideale. Un ideale in cui un elemento è invertibile coincide con tutto l'anello, mentre i divisori dello zero non contengono lo 0.

(b) segue dalla definizione di ideale.

(c) Se X ha più di un elemento, supponiamo $x, y \in X$, $x \neq y$, allora prendendo due funzioni qualsiasi f, g tali che $f(x) = 0, f(y) \neq 0, g(x) \neq 0, g(y) = 0$, abbiamo che $fg \in I(X)$ ma $f, g \notin I(X)$. Quindi $I(X)$ non è primo.
Se, invece, $X = \{x\}$, allora

$$fg \in X \Leftrightarrow f(x)g(x) = 0 \Leftrightarrow f(x) = 0 \text{ e/o } g(x) = 0 \Leftrightarrow f \in I(X) \text{ e/o } g \in I(X).$$

(d) Per il punto precedente $I(\{0\})$ è primo, però non è massimale. Infatti possiamo considerare l'omomorfismo di anelli:

$$\varphi : \mathbb{M}(\mathbb{N}, \mathbb{Z}) \to \mathbb{Z}, \quad f \mapsto f(0).$$

Si vede facilmente che φ è suriettivo (le funzioni costanti, $f(\mathbb{N}) = c$, $c \in \mathbb{Z}$, assolvono a questo compito, ad esempio) ed il nucleo è proprio $I(\{0\})$. Quindi $\mathbb{M}(\mathbb{N}, \mathbb{Z})/I(\{0\}) \cong \mathbb{Z}$, e dunque $I(\{0\})$ non è massimale (in quanto $\mathbb{M}(\mathbb{N}, \mathbb{Z})$ è un anello commutativo con unità). In particolare, si può vedere che $I(\{0\}) \subseteq \{f \in \mathbb{M}(\mathbb{N}, \mathbb{Z}) \mid f(0) \in p\mathbb{Z}\}$, dove quest'ultimo insieme è un ideale (massimale).

ESERCIZIO 4.

(a) si verifica facilmente, osservando che per la moltiplicazione bisogna utilizzare il fatto che $25 \equiv -1 \pmod{13}$.

(b) Il nucleo dell'omomorfismo è un ideale di $\mathbb{Z}[i]$ e quindi è principale e generato da un qualsiasi elemento di valutazione minima dell'ideale. Si osserva subito che $3 + 5 \cdot 2 = 13$, quindi l'elemento $3 + 2i \in ker(\varphi)$. Adesso la norma dell'elemento $3 + 2i$ è 13, quindi $3 + 2i$ è irriducibile (primo) in $\mathbb{Z}[i]$. Di conseguenza l'ideale $(3 + 2i)$ è massimale. Quindi deve per forza essere $ker(\varphi) = (3 + 2i)$, dato che già sappiamo che $(3 + 2i) \subseteq ker(\varphi)$.

(c) $\mathbb{Z}[i]/ker(\varphi) \cong \mathbb{Z}_{13}$, essendo φ suriettivo.

ESERCIZIO 5.

(a) Essendo $f_\alpha(X)$ un polinomio di terzo grado, esso è irriducibile se e solo se non ha radici. Si verifica facilmente che f_α non ha radici solo per $\alpha = 1, 2$ e questi sono i casi in cui il quoziente $\mathbb{Z}_5[X]/I_\alpha$ è un campo.

(b) Poiché $\mathbb{Z}_5[X]/I_2$ è un campo, tutte le classi non nulle sono invertibili. Quindi basta verificare che $(X^5 - X^4 + 3) \notin I_2$ per avere che la sua classe è invertibile. L'inverso si può calcolare utilizzando una qualsiasi Identià di Bezout fra f_2 e $X^5 - X^4 + 3$ (che, naturalmente, sono coprimi) e si ottiene:

$$(X^5 - X^4 + 3 + I_2)^{-1} = 4X^2 + 3 + I_2.$$