Università degli Studi Roma Tre
Corso di Laurea Triennale in Matematica, a.a. 2004/2005
AL2 - Algebra 2 - gruppi, anelli e campi
Prova di Esame - Appello A
24 gennaio 2005

Soluzione

1. Determinare le classi coniugate del gruppo diedrale D_4 delle isometrie del quadrato.

   Soluzione Ricordiamo che due elementi a e b di un gruppo G si dicono coniugati se esiste $g \in G$ tale che

   $$a = gbg^{-1}$$

   E che la classe di coniugio di un elemento a in G è

   $$\langle a \rangle = \left\{ gag^{-1}, \forall\, g \in G \right\}$$

   Ricordiamo che posto ρ la rotazione di angolo $\frac{\pi}{2}$ e σ la riflessione per l'asse x, allora possiamo scrivere

   $$D_4 = \left\{ id, \sigma, \rho, \rho^2, \rho^3, \sigma\rho, \sigma\rho^2, \sigma\rho^3 \right\}$$

   e si ha $\sigma\rho = \rho^3\sigma$. Le classi di coniugio sono

   (a) $\langle id \rangle = \{id\}$
   (b) $\langle \sigma \rangle = \{\sigma, \sigma\rho^2\} = \langle \sigma\rho^2 \rangle$
   (c) $\langle \rho \rangle = \{\rho, \rho^3\} = \langle \rho^3 \rangle$
   (d) $\langle \sigma\rho \rangle = \{\sigma\rho, \sigma\rho^3\} = \langle \sigma\rho^3 \rangle$
   (e) $\langle \rho^2 \rangle = \{\rho^2\}$

2. Determinare il gruppo $G = Aut(\mathbb{Z}_{31})$ degli automorfismi di $(\mathbb{Z}_{31}, +)$ e tutti i sottogruppi di G.

   Soluzione Ricordiamo che $\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$ omomorfismo si dice automorfismo se è biettivo, quindi si ha

$$Aut(\mathbb{Z}_n) = \{\alpha : \mathbb{Z}_n \to \mathbb{Z}_n : \alpha(1) = m \text{ con } \gcd(m, n) = 1\}$$

   Nel nostro caso

$$G = Aut(\mathbb{Z}_{31}) = \{\alpha : \mathbb{Z}_{31} \to \mathbb{Z}_{31} : \alpha(1) = m \text{ tale che } \gcd(m, 31) = 1\}$$

   Poiché 31 è primo abbiamo

$$G = \{\alpha : \mathbb{Z}_{31} \to \mathbb{Z}_{31} : \alpha(1) = m \text{ e } m \in U(\mathbb{Z}_{31})\}$$

   Allora è facile vedere che G è isomorfo a $U(\mathbb{Z}_{31})$ gruppo degli elementi invertibili di $\mathbb{Z}_{31}$, quindi $\#|G| = 30$. Poiché $U(\mathbb{Z}_{31})$ è ciclico si ha che G è ciclico e il suo generatore è α_2 definito da $\alpha_2(1) = 2$. Poiché G è ciclico abbiamo un sottogruppo per ogni divisore dell'ordine. I sottogruppi sono

   (a) (α_2^{15}) che ha ordine 2
   (b) (α_2^{10}) che ha ordine 3
   (c) (α_2^{6}) che ha ordine 5
   (d) (α_2^{5}) che ha ordine 6
   (e) (α_2^{3}) che ha ordine 10
   (f) (α_2^{2}) che ha ordine 15

3. Determinare gli ideali primi e massimali dell'anello quoziente $\dfrac{\mathbb{Z}[i]}{(6)}$.

   Soluzione

   Ricordiamo che, dato un anello A e un ideale I di A, esiste una corrispondenza biunivoca fra gli ideali massimali di A/I e gli ideali massimali di A che contengono I. Poiché $Z[i]$ è un dominio euclideo, gli ideali massimali che contengono (6) sono generati dai fattori irriducibili di 6. Quindi dobbiamo decomporre 6. Si ha che

   $$6 = 3 * 2 = 3 * (1 + i)(1 - i)$$

   Vediamo che 3 è irriducibile. Posto $N(a + bi) = a^2 + b^2$ la norma di un elemento, si ha $N(3) = 9$, ed è facile vedere che non ci sono elementi di norma 3. Quindi 3 è irriducibile. Analogamente per gli altri fattori. Dunque gli ideali massimali di $\dfrac{\mathbb{Z}[i]}{(6)}$ sono $(\overline{3})$, $(\overline{1-i})$ e $(\overline{1+i})$.

4. Si consideri l'insieme $A = \mathbb{Z}_7 \times \mathbb{Z}_7$ in cui sono definite le seguenti operazioni:

$$(a,b) + (a',b') = (a+a', b+b') \ ; \quad (a,b)(a',b') = (aa' + 5bb', ab' + a'b).$$

Rispetto a queste operazioni, A è un anello commutativo unitario con unità $1 = (1,0)$.

(a) Dimostrare che l'applicazione

$$\varphi : \mathbb{Z}_7[X] \longrightarrow A \text{ definita da } \sum a_i X^i \to \sum (a_i, 0)(0,1)^i$$

è un omomorfismo di anelli;

(b) Determinare Nucleo ed Immagine di φ ed applicare il Teorema di Omomorfismo per gli anelli;

(c) Usando il punto precedente, mostrare che A è un campo, ampliamento semplice di $\mathbb{Z}_7$, e determinare esplicitamente un elemento α di A tale che $A = \mathbb{Z}_7(\alpha)$. Quanti elementi ha A?

Soluzione

(a) Semplice verifica della definizione di omomorfismo

(b) $\operatorname{Im} \varphi = A$ e $\ker \varphi = (X^2 + 5)$, quindi il teorema di omomorfismo ci dice che $A \cong \mathbb{Z}_7[X]/(X^2+5)$

(c) Osserviamo che $X^2 + 5$ è irriducibile in $\mathbb{Z}_7[X]$, perché ha grado 2 e non ha radici, quindi l'ideale (X^2+5) è massimale. Dunque per il teorema di omomorfismo A è un campo ampliamento semplice di $\mathbb{Z}_7$ con $7^2 = 49$ elementi. Scegliamo $\alpha = (0,1)$ allora ogni elemento $(a,b) \in A$ si scrive

$$(a,b) = a(1,0) + b\alpha$$

con a e $b \in \mathbb{Z}_7$, osserviamo che $(1,0)$ è l'unità moltiplicativa di A. Quindi $A = \mathbb{Z}_7(\alpha)$