Algebra - 29 giugno 2011

Linee guida: *ogni affermazione che scrivete o utilizzate deve essere giustificata, o da un calcolo diretto, o da una dimostrazione, oppure dall'applicazione di un risultato trattato nel corso e adeguatamente citato. Il voto dipende anche dalla qualità delle spiegazioni, non solo dall'esattezza dei calcoli.*

1. Sia G un gruppo, un isomorfismo $G \xrightarrow{f} G$ è detto automorfismo. Un sottogruppo H di G è detto caratteristico se, per ogni automorfismo f, si ha:

$$f(H) \subseteq H \tag{1}$$

   - Siano $x, y \in G$, mostrare che le applicazioni $f_x(y) = xyx^{-1}$ sono automorfismi.
   - Mostrare che ogni sottogruppo caratteristico è normale.
   - Mostrare che, in ogni gruppo, il sottogruppo dei commutatori è un sottogruppo caratteristico
   - Trovare tutti gli automorfismi di $\mathbb{Z}$ e i suoi sottogruppi caratteristici.

2. Sia R un anello con unità tale che l'applicazione $f : R \to R$ data da $f(x) = x^2$ sia un omomorfismo.

   - Dimostrare che $\forall x \in R$ si ha $x + x = 0$
   - Dimostrare che l'anello R è commutativo
   - Dimostrare che $\forall y \in \ker f$, $(1 + y)$ è invertibile.

3. Considerati i tre polinomi:

$$x^2 + x + 1,\ x^2 + x + 2,\ x^2 + 2x + 2 \in \mathbb{Z}_3[x]$$

   e gli anelli gli quoziente:

$$R_1 = \frac{\mathbb{Z}_3[x]}{(x^2 + x + 1)} \tag{2}$$

$$R_2 = \frac{\mathbb{Z}_3[x]}{(x^2 + x + 2)} \tag{3}$$

$$R_3 = \frac{\mathbb{Z}_3[x]}{(x^2 + 2x + 2)} \tag{4}$$

   .

   - Quanti elementi hanno?
   - Mostrare che R_2 e R_3 sono campi e trovare esplicitamente un elemento primitivo di R_2.
   - Mostrare che invece in R_1 ci sono divisori di zero e trovarli.
   - Spiegare la ragione di questa differenza tra i tre anelli quoziente.
   - Descrivere R_1^* , R_2^* e R_3^*.
   - Dare un isomorfismo esplicito tra R_2 e R_3.

Soluzioni

Esercizio n.1

$f_x(y) = xyx^{-1}$ è un omomorfismo, è suriettivo e ha nucleo banale:

$$\begin{aligned} f_x(yz) &= xyzx^{-1} = xyxx^{-1}zx^{-1} = f_x(y)f_x(z) && (5)\\ \forall z &\in G,\ f_x(x^{-1}zx) = xx^{-1}zxx^{-1} = z && (6)\\ xyx^{-1} &= e \Rightarrow y = e \Rightarrow \ker f_x = \{e\} && (7)\end{aligned}$$

$\forall h \in H$, $\forall g \in G$ consideriamo l'automorfismo f_g; si ha allora che $ghg^{-1} = f_g(h) \in H$ per l'ipotesi che H sia caratteristico. Quindi H è normale.
Per l'ultimo punto basta osservare che il trasformato secondo un qualsiasi automorfismo di un commutatore è il commutatore dei trasformati:

$$f(xyx^{-1}y) = f(x)\, f(y)\, f\left(x^{-1}\right) f\left(y^{-1}\right) = f(x)\, f(y)\, f(x)^{-1} f(y)^{-1} \quad (8)$$

E quindi, banalmente, essendo per definizione il sottogruppo dei commutatori generato da commutatori, $f[G,G] \subseteq [G,G]$
$\mathbb{Z}$ è ciclico infinito con generatori ± 1; un automorfismo f è determinato dal valore che assume in 1, infatti

$$\begin{aligned} \text{se } n \text{ è positivo, } f(n) &= f(1) + f(1) + ... + f(1)\ n \text{ volte} && (9)\\ \text{se } n \text{ è negativo, } f(n) &= -f(1) - f(1) - ... - f(1)\ n \text{ volte} && (10)\end{aligned}$$

La suriettività richiede che i valori possibili per $f(1)$ siano solo ± 1, perchè nell'immagine ci stanno solo i multipli di $f(1)$. I due possibili automorfismi sono quindi $f_1(n) = n$ e $f_2(n) = -n$. Ogni sottogruppo è caratteristico, infatti i sottogruppi di $\mathbb{Z}$ sono del tipo $d\mathbb{Z}$ e allora:

$$f_1(dk) = dk \in d\mathbb{Z},\ f_2(dk) = -dk = d(-k) \in d\mathbb{Z} \quad (11)$$

Esercizio n.2

Se $f(x) = x^2$ è un omomorfismo di anelli unitari si deve avere:

$$\begin{aligned} f(1+x) &= f(1) + f(x) \Rightarrow (1+x)^2 = 1 + x^2 \Rightarrow 2x = 0 && (12)\\ f(x+y) &= f(x) + f(y) \Rightarrow (x+y)^2 = x^2 + y^2 \Rightarrow xy + yx = 0 && (13)\end{aligned}$$

dalla prima si ha: $2xy = 0 \Rightarrow yx = -yx$ e quindi dalla seconda $xy = yx$.
Se $y \in \ker f \Rightarrow f(y) = y^2 = 0 \Rightarrow (1+y)(1+y) = 1 + 2y + y^2 = 1$

Esercizio n.3

Sia α una radice di x^2+x+1, β una radice di x^2+x+2 e γ una radice di x^2+2x+2. Dalla teoria si sa che:

$$R_1 = \mathbb{Z}_3[\alpha] = \left\{a+b\alpha \mid a,b \in \mathbb{Z}_3,\ \alpha^2+\alpha+1=0\right\} \quad (14)$$
$$R_2 = \mathbb{Z}_3[\beta] = \left\{a+b\beta \mid a,b \in \mathbb{Z}_3,\ \beta^2+\beta+2=0\right\} \quad (15)$$
$$R_3 = \mathbb{Z}_3[\gamma] = \left\{a+b\gamma \mid a,b \in \mathbb{Z}_3,\ \gamma^2+2\gamma+2=0\right\} \quad (16)$$

Quindi i tre anelli quoziente hanno 9 elementi.
Il secondo e il terzo sono campi perchè i polinomi x^2+x+2 e x^2+2x+2 sono irriducibili (perchè di secondo grado e senza radici), mentre

$$x^2+x+1 = (2+x)(2+x) = (1+2x)(1+2x) \quad (17)$$

è riducibile.
In R_2 un elemento primitivo è, ad esempio, β. In R_1 i divisori di zero sono ovviamente $(2+\alpha)$ e $2(2+\alpha) = (1+2\alpha)$.
Per i gruppi degli elementi invertibili si ha quindi $R_1^* = \mathbb{Z}_6$ e $R_2^* = R_3^* = \mathbb{Z}_8$.
Un isomorfismo si può trovare semplicemente cercando un elemento di R_3 che sia radice del polinomio x^2+x+2. Osserviamo che:

$$\begin{aligned}(2+\gamma)^2+(2+\gamma)+2 &= 0\\ (2\gamma)^2+(2\gamma)+2 &= 0\end{aligned}$$

Gli elementi $(2+\gamma)$ e 2γ possono essere trovati con facili conti:

$$(x+\gamma y)^2+(x+\gamma y)+2=0 \Rightarrow x=2, y=1 \text{ oppure } x=0, y=2$$

Quindi gli isomorfismi possibili sono:

$$\begin{aligned}a+b\beta &\rightarrow a+2b+b\gamma\\ a+b\beta &\rightarrow a+2b\gamma\end{aligned}$$