Algebra B — 17 Marzo 2009

1. Sia f un qualsiasi omomorfismo di anelli $R_1 \xrightarrow{f} R_2$, ovvero un omomorfismo di gruppi abeliani con inoltre la proprietà $f(ab) = f(a)f(b)$ rispetto al prodotto. Supposto che R_1 e R_2 siano entrambi anelli non banali con identità 1_{R_1} e 1_{R_2}, dimostrare che:

   - Se f è suriettiva allora $f(1_{R_1}) = 1_{R_2}$
   - Se R_2 non ha divisori di zero e f è non banale, allora $f(1_{R_1}) = 1_{R_2}$
   - Trovare un omomorfismo di anelli $\mathbb{Z}_2 \xrightarrow{f} \mathbb{Z}_6$ tale che $f(1) \neq 1$
   - Trovare un omomorfismo di anelli $\mathbb{Z}_6 \xrightarrow{f} \mathbb{Z}_2$

2. Sia D_n il gruppo diedrale di ordine $2n$:

$$D_n = \left\{1, c, c^2, ..., c^{n-1}, b, bc, bc^2, ..., bc^{n-1}\right\} \text{ con } c^n = b^2 = 1, cb = bc^{-1} \tag{1}$$

   - Dimostrare che $\forall h$ intero $bc^h = c^{-h}b$
   - Dimostrare che $\forall h$ intero bc^h ha ordine 2
   - Trovare i sottogruppi di D_3 e di D_4 di ordine 2. Quali sono normali?
   - Trovare i sottogruppi di D_4 di ordine 4
   - Dimostrare che per n dispari D_n ha n sottogruppi distinti di ordine 2
   - Dimostrare che per n pari D_n ha $n+1$ sottogruppi distinti di ordine 2
   - Vero o Falso? : $D_5 \times \mathbb{Z}_3$ è isomorfo a D_{15}, $D_3 \times \mathbb{Z}_5$ è isomorfo a D_{15}, $D_5 \times \mathbb{Z}_3$ è isomorfo a $D_3 \times \mathbb{Z}_5$.

3. Sia $\mathbb{Z}_3[x]$ l'anello dei polinomi a coefficienti in $\mathbb{Z}_3$.

   - Mostrare che non ha divisori dello zero. E' un campo?
   - Fattorizzare in polinomi di primo grado il polinomio $x^2 + 2$.
   - Mostrare che il polinomio $x^2 - 2$ non ha radici in $\mathbb{Z}_3$.
   - Sia ε una soluzione formale di $x^2 - 2$ e si consideri l'insieme:

$$\mathbb{F} = \left\{a + \varepsilon b \text{ con } a, b \in \mathbb{Z}_3 \ , \ \varepsilon^2 = 2\right\} \tag{2}$$

     con le due operazioni:

$$\begin{aligned} (a + \varepsilon b) + (c + \varepsilon d) &= (a + c) + \varepsilon (b + d) & (3) \\ (a + \varepsilon b)(c + \varepsilon d) &= (ac + 2bd) + \varepsilon (ad + bc) & (4) \end{aligned}$$

     mostrare che è un campo.
   - Mostrare che, rispetto alla somma, $\mathbb{F}$ non è un gruppo ciclico.
   - Mostrare che invece rispetto alla moltiplicazione $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ è un gruppo ciclico, generato da $1 + \varepsilon$.
   - Mostrare che $\mathbb{F} = \frac{\mathbb{Z}_3[x]}{(x^2-2)}$ dove $(x^2 - 2)$ è l'ideale generato dal polinomio $x^2 - 2$.

SOLUZIONI

1. **Esercizio n.**1: ricordando le proprietà dell'identità:

$$1_{R_1} \cdot x = x \cdot 1_{R_1} = x \ \forall x \in R_1 \text{ e } 1_{R_2} \cdot y = y \cdot 1_{R_2} = y \ \forall y \in R_2 \tag{5}$$

si ha:

$$f(x) = f(1_{R_1} \cdot x) = f(1_{R_1}) \cdot f(x) \tag{6}$$
$$f(x) = f(x \cdot 1_{R_1}) = f(x) \cdot f(1_{R_1}) \tag{7}$$

- Se l'applicazione è suriettiva, $\forall y$ si ha $y = f(x)$ e quindi si ottiene $y = f(1_{R_1}) \cdot y$ e analogamente $y = y \cdot f(1_{R_1})$ e quindi per l'unicità dell'identità: $f(1_{R_1}) = 1_{R_2}$.
- Se R_2 non ha divisori di zero allora:

$$f(x) = f(1_{R_1} \cdot x) \Longrightarrow (1_{R_2} - f(1_{R_1})) \cdot f(x) = 0 \Longrightarrow (1_{R_2} - f(1_{R_1})) = 0 \tag{8}$$

- $f(0) = 0,\ f(1) = 3$;
- $f(0) = 0, f(1) = 1, f(2) = 0, f(3) = 1, f(4) = 0, f(5) = 1$

2. **Esercizio n.**2

- Si può procedere per induzione. Prima si considera il caso $h \geq 0$: la formula è vera per $h = 0$; inoltre osservato che:

$$bc = bcbb = bbc^{-1}b = c^{-1}b \tag{9}$$

Si ha:

$$bc^{h+1} = bc^h c \overset{\text{induzione!}}{=} c^{-h}bc = c^{-(h+1)}b \tag{10}$$

Il caso $h \leq 0$ segue dal caso precedente ponendo $k = -h$.

- Basta calcolare: $\left(bc^h\right)^2 = bc^h c^{-h} b = b^2 = 1$; ci sono quindi in D_n almeno n elementi di ordine 2
- D_3 ha un sottogruppo $C_3 = \{1, c, c^2\}$ di ordine 3 e 3 sottogruppi di ordine 2, $\{1, b\}, \{1, bc\}, \{1, bc^2\}$, nessuno di questi ultimi è normale.
- D_4 ha il sottogruppo $C_4 = \{1, c, c^2, c^3\}$ di ordine 4 e 5 sottogruppi di ordine 2, $\{1, c^2\}, \{1, b\}, \{1, bc\}, \{1, bc^2\}, \{1, bc^3\}$. Il sottogruppo $\{1, c^2\}$ è normale e quindi (ricordando che il prodotto NH di un sottogruppo normale N per un sottogruppo H è ancora un sottogruppo) appaiono altri 4 sottogruppi di ordine 4; di questi solo due sono distinti: $\{1, b, c^2, bc^2\}$ e $\{1, bc, c^2, bc^3\}$.
- D_n per n dispari ha, per quanto detto sopra, n elementi di ordine 2, non ce ne sono altri perché in C_n per n dispari non ce ne possono essere. D_n ha quindi n sottogruppi distinti di ordine 2 che (escluso l'elemento 1 comune a tutti) contengono complessivamente n elementi.
- In D_n per n pari anche l'elemento $c^{\frac{n}{2}}$ ha ordine 2 e quindi appare un altro sottogruppo di ordine 2, $\left\{1, c^{\frac{n}{2}}\right\}$contenuto in C_n.

- FALSO: $D_5 \times \mathbb{Z}_3$, $D_3 \times \mathbb{Z}_5$ e D_{15} hanno lo stesso numero di elementi (30) ma D_{15} ha 15 elementi di ordine 2, mentre $D_5 \times \mathbb{Z}_3$ ne ha solo 5 (perchè $\mathbb{Z}_3$ non ne ha) e $D_3 \times \mathbb{Z}_5$ ne ha solo 3 (perchè $\mathbb{Z}_5$ non ne ha).

3. **Esercizio n.**3

- $\mathbb{Z}_3[x]$ non ha divisori dello zero perchè i coefficienti sono in un campo. Non è un campo perchè gli unici elementi invertibili sono 1 e 2.
- $x^2 + 2 = (x+1)(x+2)$.
- La funzione $x^2 - 2$ assume solo i valori 1 e 2
- E' un campo perchè è un anello commutativo con unità ed inoltre si mostra che ogni elemento diverso da zero ha un *inverso.* Si consideri il prodotto:

$$(a + \varepsilon b)(a - \varepsilon b) = a^2 - 2b^2 \tag{11}$$

  In $\mathbb{Z}_3$, se $a \neq 0$ e $b \neq 0$, si ha $a^2 - 2b^2 = 1 - 2 = -1$ (in virtù del teorema di Fermat) e quindi ogni elemento con $a \neq 0$ e $b \neq 0$ ha un inverso:

$$(a + \varepsilon b)^{-1} = -a + \varepsilon b \tag{12}$$

  Gli altri elementi diversi da zero hanno invece come inversi: $a^{-1} = a$ e $(\varepsilon b)^{-1} = 2\varepsilon b$, infatti $a^2 = 1$ e $(\varepsilon b)(2\varepsilon b) = 4b^2 = 1$ ancora per Fermat.
- $\mathbb{F}$ ha ordine 9, ma non ha elementi di ordine 9, infatti per tutti i suoi elementi si ha: $3(a + \varepsilon b) = 0$.
- $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ ha ordine 8, e quindi basta trovare un elemento di ordine 8. Osserviamo che ε ha ordine 4 e che $(1+\varepsilon)^2 = 2\varepsilon$ e quindi $(1+\varepsilon)^4 = 2$, e allora $(1+\varepsilon)$ ha necessariamente ordine 8, quindi è un generatore e il gruppo è ciclico.
- In $\mathbb{F} = \frac{\mathbb{Z}_3[x]}{(x^2-2)}$ ogni classe è rappresentata da $\overline{a + bx}$, essendo $a + bx$ il resto della divisione di qualsiasi polinomio per $x^2 - 2$. Basta verificare che la somma e il prodotto tra classi sono gli stessi definiti più sopra da:

$$\begin{aligned} (a + \varepsilon b) + (c + \varepsilon d) &= (a + c) + \varepsilon(b + d) && (13) \\ (a + \varepsilon b)(c + \varepsilon d) &= (ac + 2bd) + \varepsilon(ad + bc) && (14) \end{aligned}$$

  Per la somma è ovvio, per il prodotto si ha:

$$\left(\overline{a + bx}\right)\left(\overline{c + dx}\right) = \overline{(a + bx)(c + dx)} = \overline{ac + (ad + bc)x + bdx^2} \tag{15}$$

  ma essendo:

$$ac + (ad + bc)x + bdx^2 = ac + 2bd + x(ad + bc) + bd\left(x^2 - 2\right) \tag{16}$$

  si ottiene il risultato voluto:

$$\left(\overline{a + bx}\right)\left(\overline{c + dx}\right) = \overline{ac + 2bd + x(ad + bc)} \tag{17}$$