Algebra B — 1 Aprile 2009

1. Sia $\omega \neq 1$ una radice cubica complessa di 1 e sia $\mathbb{Z}[\omega] = \{a + \omega b \mid a, b \in \mathbb{Z}\}$ (gli elementi di $\mathbb{Z}[\omega]$ sono detti "interi di Eisenstein")

   - Mostrare che ω soddisfa l'equazione $\omega^2 + \omega + 1 = 0$
   - Mostrare che $\mathbb{Z}[\omega]$ è un anello commutativo con indentità definendo in $\mathbb{Z}[\omega]$ una somma e un prodotto "naturali".
   - Mostrare che i sei elementi $\pm 1, \pm\omega, \pm(1+\omega)$ sono unità dell'anello $\mathbb{Z}[\omega]$
   - Mostrare che $G = \{\pm 1, \pm\omega, \pm(1+\omega)\}$ con il prodotto definito in $\mathbb{Z}[\omega]$ è un gruppo abeliano ciclico.
   - Mostrare esplicitamente, scrivendo un isomorfismo, che G è isomorfo a $\mathbb{Z}_6$.
   - Trovare[1] $\mathbb{Z}[\omega]^*$ cioè il gruppo degli elementi invertibili di $\mathbb{Z}[\omega]$.
   - Mostrare che ogni $z = a + \omega b \in \mathbb{Z}[\omega]$ è radice del polinomio

     $$z^2 - (2a - b)z + (a^2 - ab + b^2)$$

   - Mostrare che $\mathbb{Z}[\omega]$ è isomorfo a $\frac{\mathbb{Z}[x]}{(x^2+x+1)}$ dove $(x^2 + x + 1)$ è l'ideale generato dal polinomio $x^2 + x + 1$.

2. Sia G un gruppo e H un suo sottogruppo. Si consideri l'insieme $N(H)$:

   $$N(H) = \left\{x \in G \text{ tali che } xHx^{-1} = H\right\}$$

   - Si mostri che $N(H)$ è un sottogruppo di G.
   - Si mostri che $N(H) = G$ se e solo se H è normale in G.
   - Supposto ora G di ordine finito, si mostri che l'ordine di $N(H)$ è un multiplo dell'ordine di H.

[1] Per risolvere questo punto usare il fatto che le uniche soluzioni **intere** dell'equazione $a^2 + b^2 - ab = 1$ sono: $a = \pm 1, b = 0$; $a = 0, b = \pm 1$; $a = b = \pm 1$. Invece l'equazione $a^2 + b^2 - ab = -1$ non ammette soluzioni intere.

Questo può essere dimostrato facilmente risolvendo esplicitamente ad esempio per l'incognita a e analizzando le condizioni per cui le soluzioni siano intere

SOLUZIONI

1. **Esercizio n.**1

   - $\omega^3 = 1$ per cui abbiamo:

     $$S = 1 + \omega + \omega^2 = \omega + \omega^2 + \omega^3 = \omega(1 + \omega + \omega^2) = \omega S$$

     essendo $\omega \neq 1$ segue $S = 0$
   - Le operazioni naturali sono:

     $$\begin{aligned} (a + \omega b) + (c + \omega d) &= (a + c) + \omega\,(b + d) && (1)\\ (a + \omega b) \cdot (c + \omega d) &= ac + ad\omega + bc\omega + bd\omega^2 = && (2)\\ ac + ad\omega + bc\omega + bd(-1 - \omega) &= ac - bd + \omega\,(ad + bc - bd) && (3) \end{aligned}$$

     queste operazioni sono interne all'insieme, associative, distributive e commutative, gli elementi neutri sono rispettivamente $0, 1$.
   - Gli elementi dati sono invertibili, infatti:

     $$\begin{aligned} (\pm 1)^{-1} &= \pm 1\\ (\pm\omega)^{-1} &= \pm\omega^2 = \mp(1 + \omega) \quad \text{(ricordando che } \omega^3 = 1) \end{aligned}$$

   - Il gruppo G è ciclico di ordine 6, infatti si trova subito che, ad esempio, $-\omega$ è un generatore:

     $$\begin{aligned} (-\omega)^1 &= -\omega\\ (-\omega)^2 &= \omega^2 = -1 - \omega\\ (-\omega)^3 &= -\omega^3 = -1\\ (-\omega)^4 &= \omega^4 = \omega^3\omega = \omega\\ (-\omega)^5 &= -\omega^5 = -\omega^3\omega^2 = -\omega^2 = 1 + \omega\\ (-\omega)^6 &= \omega^6 = \left(\omega^3\right)^2 = 1 \end{aligned}$$

   - Un isomorfismo $f : \mathbb{Z}_6 \to \mathbb{Z}\,[\omega]$ si ottiene, ad esempio, mandando il generatore 1 nel generatore $-\omega$, ovvero $f(n) = (-\omega)^n$ con $n = 0, 1, 2, 3, 4, 5 \in \mathbb{Z}_6$.
   - Si consideri l'equazione:

     $$(a + \omega b) \cdot (x + \omega y) = ax - by + \omega\,(ay + bx - by) = 1 \qquad (4)$$

     Con a, b interi non contemporaneamente nulli. Si ottiene il sistema:

     $$\begin{aligned} ax - by &= 1\\ (ay + bx - by) &= 0 \end{aligned}$$

     dove deve essere anche $a, b, x, y \in \mathbb{Z}$. Il sistema ammette le soluzioni formali:

     $$\begin{aligned} x &= \frac{a - b}{a^2 + b^2 - ab}\\ y &= \frac{-b}{a^2 + b^2 - ab} \end{aligned}$$

Il denominatore (il determinante della matrice del sistema) non può mai essere zero se $a, b \in \mathbb{Z}$ e non contemporaneamente nulli (infatti risolvendo esplicitamente l'equazione $a^2+b^2-ab=0$ come equazione di secondo grado in a, si ottiene subito che il discriminante è $-3b^2$ e quindi non ci sono soluzioni reali e tantomeno intere). Questo fatto dimostra anche subito che l'anello non ha divisori di zero. Ci sono ora tre casi.

(a) Se $b=0$, $y=0$ e affinchè anche $x=\frac{1}{a}$ sia intero deve essere $a=\pm 1$ e quindi ± 1 sono elementi invertibili.

(b) Se $a=0$, $x=y=-\frac{1}{b}$ e allora affinchè x e y siano interi deve essere $b=\pm 1$ e quindi $\pm\omega$ sono elementi invertibili con inversi rispettivamente $\mp(1+\omega)$

(c) Se a e b sono ambedue diversi da zero, affinchè x e y siano interi deve essere $a^2+b^2-ab=1$ oppure $a^2+b^2-ab=-1$ (che però è impossibile). Nel primo caso, $a^2+b^2-ab-1=0$, le soluzioni formali (ad esempio per a) sono:

$$\frac{1}{2}b-\frac{1}{2}\sqrt{4-3b^2}, \frac{1}{2}b+\frac{1}{2}\sqrt{4-3b^2}$$

E queste sono reali, intere e diverse da zero (cioè vere soluzioni) solo per $b=\pm 1$ che a sua volta fornisce $a=\pm 1$. Risulta quindi che $\pm(1+\omega)$ sono elementi invertibili.

(d) Riassumendo, non essendoci altri casi, gli elementi invertibili sono solo:

$$\{\pm 1, \pm\omega, \pm(1+\omega)\}$$

(e)

$$a^2-ab+b^2+(a+b\omega)^2-(a+b\omega)(2a-b)=b^2+b^2\omega+b^2\omega^2=b^2 0=0$$

- In $\frac{\mathbb{Z}[x]}{(x^2+x+1)}$ ogni classe è rappresentata da $\overline{a+bx}$, essendo $a+bx$ il resto della divisione di qualsiasi polinomio per x^2+x+1. Basta verificare che la somma e il prodotto tra classi sono gli stessi definiti più sopra da:

$$\begin{aligned}(a+\omega b)+(c+\omega d) &= (a+c)+\omega(b+d) &(5)\\ (a+\omega b)\cdot(c+\omega d) &= ac-bd+\omega(ad+bc-bd) &(6)\end{aligned}$$

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

$$\left(\overline{a+bx}\right)\left(\overline{c+dx}\right)=\overline{(a+bx)(c+dx)}=\overline{ac+(ad+bc)x+bdx^2} \qquad (7)$$

ma essendo:

$$ac+(ad+bc)x+bdx^2=(x^2+x+1)bd+(ad+bc-bd)x+ac-bd \qquad (8)$$

si ottiene il risultato voluto:

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