Università degli studi di Roma Tre
Corso di Laurea Triennale in Matematica, a.a. 2003/2004
AL2 - Algebra 2, gruppi anelli e campi
Soluzioni
21 Novembre 2004

1 Definizione di Anello

1. *Binomio* Sia R un anello. Siano a e $b \in R$, allora:
   (a) Dimostrare che $(a+b)^2 = a^2 + ab + ba + b^2$.
   (b) Trovare la forma del teorema del binomio in R; trovare cioè un'espressione per $(a+b)^n$, con n intero positivo.

   Soluzione 1.1. *(a) Usiamo la distributività,*
   $$(a+b)^2 = (a+b)(a+b) = a(a+b) + b(a+b) = a^2 + ab + ba + b^2$$
   (b)
   $$(a+b)^n = \sum_{i=(i_0,\cdots,i_n)} a^{i_0} b^{i_1} \cdots b^{i_{n-1}} a^{i_n}$$
   tale che $i_0 + \cdots + i_n = n$.

2. Sia $R = \{A = (a_{ij}) \in M_n(\mathbb{R}) : a_{ij} = 0 \text{ se } i < j\}$. Dimostrare che R è un sottoanello unitario di $M_n(\mathbb{R})$.

   Soluzione 1.2. *Bisogna verificare che* $\forall A, B \in R : A+B \in R$ *e* $AB \in R$. *La prima è ovvia, la seconda si ottiene applicando la definizione di prodotto riga per colonna. L'unità di R è* $I = (a_{ij}) : a_{ii} = 1$ *e* $a_{ij} = 0$ *per* $i \neq j$.

3. Sia $R = \{A = (a_{ij}) \in M_n(\mathbb{R}) : a_{ij} = 0 \text{ se } i \leq j\}$. Dimostrare che R è un sottoanello di $M_n(\mathbb{R})$. R è unitario ?

   Soluzione 1.3. *Bisogna verificare che* $\forall A, B \in R : A+B \in R$ *e* $AB \in R$. *La prima è ovvia, la seconda si ottiene applicando la definizione di prodotto riga per colonna. R non è unitario.*

4. Sia $R = \{A = (a_{ij}) \in M_3(\mathbb{R}) : a_{ij} = 0 \text{ se } i = 2 \text{ o } j = 2\}$. Dimostrare che R è un sottoanello di $M_3(\mathbb{R})$. R è unitario ?

   Soluzione 1.4. *Bisogna verificare che* $\forall A, B \in R : A+B \in R$ *e* $AB \in R$. *La prima è ovvia, la seconda si ottiene applicando la definizione di prodotto riga per colonna. L'unità di R è* $I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

5. Sia $R = \{a = (a_n)_{n\in\mathbb{N}} : a_n \in \mathbb{Q}$ e a_n quasi tutti nulli$\}$. Per ogni a e $b \in R$ definiamo

   - $a + b = (a_n + b_n)_{n\in N}$
   - $a \cdot b = (a_n b_n)_{n\in\mathbb{N}}$

   Verificare se R è un anello.

   Soluzione 1.5. *Semplice verifica degli assiomi.*

2 Ideali

1. Sia R un anello, I un ideale di R e $1 \in I$ allora $I = R$

   Soluzione 2.1. *Ricordiamo che se I è un anello allora, $\forall a \in I$ e $\forall b \in R$: $ba \in I$. Poiché $1 \in I$ allora,$\forall a \in R$, $a = a \cdot 1 \in I$.*

2. Sia R un anello commutativo e $a \in R$

   (a) dimostrare che $aR = \{ar : r \in R\}$ è un ideale bilatero di R.

   (b) dimostrare con un esempio che ciò può non essere vero se R non è commutativo.

   Soluzione 2.2. *(a) aR è un idela destro per definizione, poichè R è commutativo, ogni ideale destro è anche un ideale sistro.*

   (b) Consideriamo $R = M_2(\mathbb{R})$, $a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Allora

   $$aR = \{A = (a_{ij}) : a_{2j} = 0 \forall j\}$$

   che è un ideale destro ma non sinistro.

3. Dimostrare che tutti gli ideali di $\mathbb{Z}$ sono della forma $n\mathbb{Z}$.

   Soluzione 2.3. *Sappiamo che un ideale di un anello R è anche un sottogruppo additivo. I sottogruppi additivi di $\mathbb{Z}$ sono $n\mathbb{Z}$, per cui tutti gli ideali di $\mathbb{Z}$ sono della forma $n\mathbb{Z}$. É facile verificare che ogni $n\mathbb{Z}$ è un ideale.*

4. Dimostrare che $n\mathbb{Z}$ è un ideale primo se e solo se n è primo o $n = 0$.

   Soluzione 2.4. *Supponiamo I primo non nullo. Allora $I = n\mathbb{Z}$ per qualche n.*

   $$I \text{ primo} \Rightarrow \forall a \text{ e } b \in R : ab \in I \text{ allora } a \in I \text{ o } b \in I.$$

   La seconda parte ci dice che:

   $$\forall a \text{ e } b \in \mathbb{Z} : n|ab \Rightarrow n|a \text{ o } n|b.$$

   Dunque n è primo. Il viceversa è ovvio.

5. Sia I un ideale di $\mathbb{Z}$ non nullo. Dimostrare che I è primo $\Leftrightarrow$ I è massimale.

Soluzione 2.5. *Usiamo la seguente caratterizzazione degli ideali massimali:*

$$I \text{ è massimale } \Leftrightarrow R/I \text{ è un campo.}$$

Grazie all'esercizio 4 sappiamo che I è primo non nullo $\Leftrightarrow I = p\mathbb{Z}$ con p primo. Dunque

$$\mathbb{Z}/I = \mathbb{Z}/p\mathbb{Z} \text{ è un campo} \Rightarrow I \text{ è massimale.}$$

Il viceversa è sempre vero, ogni ideale massimale è primo.

6. *Teorema Cinese dei resti* Siano $I_1, \cdots, I_n$ ideali di R, anello commutativo con identità, tali che $I_i + I_j = R$ per ogni $i \neq j$. Siano $x_1, \cdots, x_n \in R$, allora esiste $x \in R$ tale che $x \equiv x_i \mod I_i$. Verificare che per $R = \mathbb{Z}$ si ottiene l'usuale teorema cinese dei resti.

Soluzione 2.6. *Dimostriamolo per induzione. Se $n = 2$, abbiamo*

$$1 = a_1 + a_2$$

per qualche elemento $a_i \in I_i$, e poniamo $x = x_2a_1 + x_1a_2$. Per $i \geq 2$, possiamo trovare degli elementi $a_i \in a_1$ e $b_i \in a_i$ tali che

$$1 = a_i + b_i, \ \forall i \geq 2.$$

Il prodotto $\prod_{i=2}^n a_i + b_i$ è uguale ad 1, e vive in $I_1 + \prod_{i=2}^n I_i$. Dunque

$$I_1 + \prod_{i=2}^{n} I_i = A.$$

Grazie al teorema per $n = 2$, esiste $y_1 \in A$ tale che

$$\begin{aligned} y_1 &\cong 1 \mod I_1 &(1)\\ y_1 &\cong 0 \mod \prod_{i=2}^{n} I_i &(2) \end{aligned}$$

Per induzione esistono $y_2 \cdot y_n$ tali che

$$\begin{aligned} y_i &\cong 1 \mod I_i &(3)\\ y_i &\cong 0 \mod I_j \, i \neq j. &(4) \end{aligned}$$

Allora $x = x_1y_1 + \cdot + x_ny_n$ è l'elemento cercato.

7. Consideriamo

(a) $\mathbb{Z}_{30}$ e $R = \{\overline{0}, \overline{6}, \overline{12}, \overline{18}, \overline{24}\} \subset \mathbb{Z}_{30}$.

(b) $\mathbb{Z}_{20}$ e $R = \{\overline{0}, \overline{5}, \overline{10}, \overline{15}\} \subset \mathbb{Z}_{20}$.

Verificare, in entrambi i casi, se R è un sottoanello, ha divisori dello zero, ed è un campo. Trovare un anello ad esso isomorfo.

Soluzione 2.7. *(a)* $\{\overline{0}, \overline{6}, \overline{12}, \overline{18}, \overline{24}\}$ *è un sottoanello, non ha divisori dello zero, è un campo ed è isomorfo a* $\mathbb{Z}_5$.

(b) $\{\overline{0}, \overline{5}, \overline{10}, \overline{15}\}$ *è un sottoanello, ha divisori dello zero* $10 * 10 = 100 = 0 \mod 20$*, dunque non è un campo ed è isomorfo* $\mathbb{Z}_4$*.*