Università degli studi di Roma Tre
Corso di Laurea Triennale in Matematica, a.a. 2004/2005
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.*

6. Un elemento a di un anello A si dice *nilpotente* se $a^k = 0$ per qualche $k \geq 1$.

   Mostrare che, se $n = p_1^{k_1} \dots p_s^{k_s}$ è la fattorizzazione di n in numeri primi, allora $\overline{a} \in \mathbb{Z}_n$ è nilpotente se e soltanto se p_i divide a per $i = 1, \dots, s$.

   Da questo fatto, dedurre che, se p è primo, ogni elemento di $\mathbb{Z}_{p^k}$ è invertibile oppure nilpotente.

   Soluzione 1.6. *Osserviamo che per ogni i $\overline{p_i}$ è uno zero divisore di $\mathbb{Z}_n$. Supponiamo che $p_i|a$ per $i = 1 \dots s$ allora*

   $$a = p_1^{h_1} \dots p_s^{h_s}$$

   Allora

   $$a^{k_1 \dots k_n} = 0$$

   Quindi a è nilpotente. Sia $a \in \mathbb{Z}_{p^k}$ con p primo, allora

   $$\gcd(a, p) = 1 \text{ o } p|a$$

   Quindi a è invertibile o nilpotente.

7. Sia $\mathcal{S}$ un insieme non vuoto e sia $P(\mathcal{S})$ l'insieme delle parti di $\mathcal{S}$. Definiamo in $P(\mathcal{S})$ le seguenti operazioni:

   $$\mathcal{X} + \mathcal{Y} = (\mathcal{X} \cup \mathcal{Y}) \setminus (\mathcal{X} \cap \mathcal{Y})(\textit{differenza simmetrica}); \mathcal{X}\mathcal{Y} = (\mathcal{X} \cap \mathcal{Y}).$$

   Mostrare che:

   (a) $(P(\mathcal{S}), +, \cdot)$ è un anello commutativo unitario (dare per scontato che le operazioni sono associative e che vale la proprietà distributiva);

   (b) Ogni elemento di $P(\mathcal{S})$ diverso da 0 e 1 è uno zerodivisore;

   (c) Ogni elemento di $P(\mathcal{S})$ coincide con il suo opposto ed è idempotente;

   (d) $(P(\mathcal{S}), +, \cdot)$ è un campo se soltanto se $\mathcal{S}$ ha un solo elemento;

(e) L'insieme $P_{fin}(\mathcal{S})$ dei sottoinsiemi finiti di $\mathcal{S}$ è un ideale di $P(\mathcal{S})$;

(f) Per ogni sottoinsieme proprio $\mathcal{X}$ di $\mathcal{S}$, $P(\mathcal{X})$ è un sottoanello di $P(\mathcal{S})$. Inoltre $P(\mathcal{X})$ è unitario, ma la sua unità è differente da quella di $P(\mathcal{S})$;

(g) Per ogni sottoinsieme $\mathcal{X}$ di $\mathcal{S}$, $P(\mathcal{X})$ è un ideale principale di $P(\mathcal{S})$.

Soluzione 1.7.

(a) Semplice verifica

(b) Sia $\mathcal{X} \neq 0$ allora $\mathcal{X}(\mathcal{S} \setminus \mathcal{X}) = 0$

(c) Segue dalla definizione delle operazioni

(d) Se $\mathcal{S}$ ha un solo elemento allora $P(\mathcal{S}) = \{0, 1\}$ è un campo. Se $\mathcal{S}$ ha più di due elementi allora per il punto b $P(\mathcal{S})$ non può esere un campo perchè ha zero divisori.

(e) Semplice verifica

(f) Semplice verifica. Inoltre l'unità di $P(\mathcal{X})$ è $\mathcal{X}$ mentre quella di $P(\mathcal{S})$ è $\mathcal{S}$

(g) Semplice verifica

8. In $\mathbb{Z}_{28}$ il sottoannello $\langle \overline{4} \rangle$ è un campo.

Soluzione 1.8.

$$\langle \overline{4} \rangle = \left\{ \overline{0}, \overline{4}, \overline{8}, \overline{12}, \overline{16}, \overline{20}, \overline{24} \right\}$$

Verifichiamo che è un campo. Osserviamo che l'unità è $\overline{8}$. Il resto delle proprietà sono una semplice verifica.

2 Divisioni in $\mathbb{Q}[x]$ e $\mathbb{Z}[x]$

1. Consideriamo le seguenti coppie di polinomi in $\mathbb{Q}[x]$

- $f = 3x + 2$ e $g = x^3 + 3x + 2$
- $f = x + 1$ e $g = x^2 + 5x + 1$
- $f = x^2 + 2x + 3$ e $x^3 + 3x^2 + 3x + 8$
- $f = 6x + 5$ e $g = x^3 + 4x^2 + 5x + 1$

Calcolare il quoziente e il resto della divisione di g rispetto a f.

Soluzione 2.1.

- $q(x) = \frac{1}{3}x^2 - \frac{2}{9}x + \frac{31}{27}$ *e* $r(x) = \frac{19}{27}$
- $q(x) = x + 4$ *e* $r(x) = -3$

- $q(x) = 1 + x$ *e* $r(x) = -2x + 5$
- $q(x) = \frac{1}{6}x^2 + \frac{19}{36}x + \frac{85}{216}$ *e* $r(x) = -\frac{209}{216}$

2. Consideriamo le seguenti coppie di polinomi in $\mathbb{Z}[x]$

   - $f = x + 2$ e $g = x^3 + 3x + 2$
   - $f = x + 1$ e $g = x^2 + 5x + 2$
   - $f = x^2 + x + 1$ e $4x^3 + 3x^2 + 2x + 1$
   - $f = 2x + 4$ e $g = 2x^3 + 3x^2 + 5x + 1$
   - $f = 2x + 3$ e $g = x^2 + 2x - 1$

   Calcolare il quoziente e il resto della divisione di g rispetto a f.

   Soluzione 2.2.

   - $q(x) = x^2 - 2x + 7$ *e* $r(x) = -12$
   - $q(x) = x + 4$ *e* $r(x) = -2$
   - $q(x) = 4x - 1$ *e* $r(x) = -x + 2$
   - $q(x) = x^2 - \frac{1}{2}x + \frac{7}{2}$ *e* $r(x) = -13$ *non è divisibile in* $\mathbb{Z}[x]$
   - $q(x) = \frac{1}{2}x + \frac{1}{4}$ *e* $r(x) = -\frac{7}{4}$ *non è divisibile in* $\mathbb{Z}[x]$

3. Calcolare il massimo comun divisore fra le seguenti coppie di polinomi in $\mathbb{Q}[x]$

   - $x^3 + 3x + 2$ e $x^4 + x^2 + 1$
   - $x^2 + 3x + 2$ e $x + 1$
   - $5x^3 + 4x^2 + 3x + 3$ e $2x^2 + 2x + 2$
   - $5x^2 + 3$ e $x^2 + x + 1$

   Soluzione 2.3. *Il massimo comun divisore è*

   - *1*
   - $x + 1$
   - *1*
   - *1*

3 Divisione in $\mathbb{Z}_p[x]$ con p primo

1. Consideriamo le seguenti coppie di polinomi in $\mathbb{Z}_5[x]$

   - $f = x + 2$ e $g = x^3 + 3x + 2$
   - $f = x + 1$ e $g = x^2 + 5x + 2$

- $f = x^2 + x + 1$ e $4x^3 + 3x^2 + 2x + 1$
- $f = 2x + 4$ e $g = 2x^3 + 3x^2 + 5x + 1$
- $f = 2x + 3$ e $g = x^2 + 2x - 1$

Calcolare il quoziente e il resto della divisione di g rispetto a f.

Soluzione 3.1.

- $q(x) = x^2 + 3x + 2$ *e* $r(x) = 3$
- $q(x) = x + 4$ *e* $r(x) = 3$
- $q(x) = 4x + 4$ *e* $r(x) = 4x + 2$
- $q(x) = x^2 + 2x + 1$ *e* $r(x) = 2$ *non è divisibile in* $\mathbb{Z}[x]$
- $q(x) = 3x + 4$ *e* $r(x) = 4$ *non è divisibile in* $\mathbb{Z}[x]$

2. Calcolare il massimo comun divisore fra le seguenti coppie di polinomi in $\mathbb{Z}_5[x]$

   - $x^3 + 3x + 2$ e $x^4 + x^2 + 1$
   - $x^2 + 3x + 2$ e $x + 1$
   - $5x^3 + 4x^2 + 3x + 3$ e $2x^2 + 2x + 2$
   - $5x^2 + 3$ e $x^2 + x + 1$

   Soluzione 3.2. *Il massimo comun divisore è*

   - *1*
   - $x + 1$
   - *1*
   - *1*

4 Relazioni di Equivalenza

1. Consideriamo $A = \mathbb{Q}[x]$, definiamo la se seguente relazione, per ogni f e $g \in A$

   $$f \approx g \Leftrightarrow x | f - g$$

   Dimostrare che $\approx$ è una relazione di equivalenza, descrivere le classi di equivalenza.

   Soluzione 4.1. $\approx$ *è una relazione di equivalenza se verifica le seguenti proprietà*

   - *Riflessiva:* $f \approx f$
   - *Simmetrica:* $f \approx g \Rightarrow g \approx f$

- *Transitiva:* $f \approx g$ *e* $g \approx h \Rightarrow f \approx h$

Verifichiamole

- *Riflessiva:* $x|0 = f - f$ *dunque* $f \approx f$
- *Simmetrica:* $f \approx g$ *allora* $x|f - g$ *da cui* $f - g = x \cdot h$ *per qualche* $h \in \mathbb{Q}[x]$. *Allora*
$$g - f = -(f - g) = -x \cdot h = x \cdot (-h) \Rightarrow x|g - f$$
- *Transitiva:* $f \approx g$ *e* $g \approx h$ *quindi* $x|f - g$ *e* $x|g - h$, *ma* $f - h = (f - g) + (g - h)$ *dunque* $x|f - h$.

2. Consideriamo $A = \mathbb{R}[x]$, definiamo la se seguente relazione, per ogni f e $g \in A$
$$f \approx g \Leftrightarrow x^2 + 1|f - g$$
Dimostrare che $\approx$ è una relazione di equivalenza, descrivere le classi di equivalenza.

Soluzione 4.2. *Si verifica facilmente che* $\approx$ *è una relazione di equivalenza. Descriviamo le classi di equivalenza. Sia*
$$\begin{aligned} f(x) &= q(x)(x^2 + 1) + r(x) \\ g(x) &= q'(x)(x^2 + 1) + r'(x) \end{aligned}$$
Allora $f \approx g \Leftrightarrow r(x) = r'(x)$, *notiamo che* $r(x)$ *ha grado al più* 1, *perché è il resto della divisione per* $x^2 + 1$.
$$\overline{f} = \left\{a + bx + (x^2 + 1)h(x)\colon\ h(x) \in \mathbb{R}[x]\right\} = \overline{a + bx}$$
Quindi possiamo definire $\gamma : \mathbb{R}[x]/ \approx \to \mathbb{C}$ $\gamma(\overline{a + bx}) = a + bi$. *Si verifica facilmente che* γ *è un isomorfismo di insiemi. Si noti che* $\approx$ *è compatibile con la somma e il prodotto di* $\mathbb{R}[x]$ *quindi* γ *è un omomorfismo.*

5 Anello dei polinomi

1. Sia A un anello. Mostrare che il polinomio $u + aX \in A[X]$ è invertibile se e soltanto se u è invertibile ed a è nilpotente.

Determinare poi esplicitamente l'inverso del polinomio $\overline{5} + \overline{6}X \in \mathbb{Z}_{12}[X]$

Soluzione 5.1. *Supponiamo che* $u + aX$ *sia invertibile, allora esiste un polinomio non nullo di grado* n $p(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$ *tale che* $(u + aX)p(X) = 1$, *da cui*
$$\begin{aligned} &ua_0 = 1 \\ &ua_i + aa_{i-1} = 0 \text{ \textit{per ogni} } i = 1 \dots n \\ &aa_n = 0 \end{aligned}$$

Da cui $a_i = (-1)^i u^{-(i+1)} a^i$ *per* $i = 1 \dots n$. *Quindi* u *è invertibile e* $a^{n+1} = 0$. *Viceversa se* u *è invertibile e* a *è nilpotente tale che* $a^{n+1} = 0$ *allora*

$$p(X) = u^{-1} + \sum_{i=1}^{n} (-1)^i u^{-(i+1)} a^i X^i$$

è l'inverso. Inoltre l'inverso di $\overline{5} + \overline{6}X$ *è* $\overline{5} + \overline{6}X$