Università degli Studi Roma Tre
Corso di Laurea Triennale in Matematica, a.a. 2002/2003
AL2 - algebra 2, gruppi, anelli e campi
Tutorato - Soluzioni
18 novembre 2003

1. Si consideri il seguente sottoinsieme del corpo dei quaternioni reali $\mathbf{H}(\mathbb{R})$:

$$\mathbf{H}(\mathbb{Z}) = \{a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \quad | \quad a, b, c, d \in \mathbb{Z}\}.$$

1. Verificare che $\mathbf{H}(\mathbb{Z})$ è un sottoanello di $\mathbf{H}(\mathbb{R})$ unitario, non commutativo e privo di divisori dello zero.
2. Determinare gli elementi invertibili di $\mathbf{H}(\mathbb{Z})$.
3. Se $\mathbf{q} = 3\mathbf{1} - 2\mathbf{j}$ e $\mathbf{q}' = -1\mathbf{1} + 1\mathbf{i} - 2\mathbf{k}$, trovare $\mathbf{q} + \mathbf{q}'$, $\mathbf{q}\mathbf{q}'$ e $\mathbf{q}^{-1}$.

1. $\mathbf{H}(\mathbb{Z})$ è un sottoanello unitario di $\mathbf{H}(\mathbb{R})$ dato che $\forall \mathbf{q}, \mathbf{q}' \in \mathbf{H}(\mathbb{Z})$ $\mathbf{q} - \mathbf{q}' \in \mathbf{H}(\mathbb{Z})$, $\mathbf{q}\mathbf{q}' \in \mathbf{H}(\mathbb{Z})$ e l'unità di $\mathbf{H}(\mathbb{R})$, $\mathbf{1}$, appartiene a $\mathbf{H}(\mathbb{Z})$.
   $\mathbf{H}(\mathbb{Z})$ non è commutativo dato che $\mathbf{ij} = \mathbf{k}$ mentre $\mathbf{ji} = -\mathbf{k}$
   Infine $\mathbf{H}(\mathbb{Z})$ è privo di divisori dello zero visto che è un sottoanello di un corpo (si ricordi che gli elementi invertibili non possono essere zero-divisori).
2. Sia $\mathbf{q} = a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbf{H}(\mathbb{Z})$, $\mathbf{q} \neq 0$. Siccome $\mathbf{H}(\mathbb{Z})$ è un sottoanello unitario di $\mathbf{H}(\mathbb{R})$, e l'inverso di un elemento è unico, si ha che: $\mathbf{q}$ è invertibile in $\mathbf{H}(\mathbb{Z}) \Leftrightarrow \mathbf{q}^{-1}$ (inverso in $\mathbf{H}(\mathbb{R})$) $\in \mathbf{H}(\mathbb{Z})$
   $\mathbf{q}^{-1} = \overline{\mathbf{q}}/N(\mathbf{q})$ con $N(\mathbf{q}) = a^2 + b^2 + c^2 + d^2$. Siccome $\mathbf{q} \neq 0$ possiamo supporre $a \neq 0$ (negli altri casi si procede analog.). $\mathbf{q}$ invertibile in $\mathbf{H}(\mathbb{Z}) \Rightarrow N(\mathbf{q})|a \Rightarrow a = \pm 1,\ b = 0,\ c = 0,\ d = 0$. Inoltre se $a = \pm 1,\ b = 0,\ c = 0,\ d = 0$ chiaramente $N(\mathbf{q})$ divide a, b, c, d.
   Concludendo: gli elementi invertibili di $\mathbf{H}(\mathbb{Z})$ sono $\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}$.
3. $\mathbf{q} + \mathbf{q}' = 2\mathbf{1} + 1\mathbf{i} - 2\mathbf{j} - 2\mathbf{k}$
   $\mathbf{q}\mathbf{q}' = -3\mathbf{1} + 7\mathbf{i} + 2\mathbf{j} - 4\mathbf{k}$
   $\mathbf{q}^{-1} = \frac{3}{13}\mathbf{1} + \frac{2}{13}\mathbf{j}$.

2. Sia A un anello ed $a \in A$; a si dice
- *idempotente* se $a^2 = a$;
- *nilpotente* se esiste $n > 0$ tale che $a^n = 0$.

1. Provare che se a è nilpotente e $a \neq 0$, allora a è zero-divisore.
2. Provare che se A è unitario ed a è idempotente con $a \neq 0$ e $a \neq 1$, allora a è zero-divisore.
3. Dare l'esempio di un elemento $\neq 0$ nilpotente e non idempotente.
4. Dare l'esempio di un elemento $\neq 0$ e $\neq 1$ idempotente e non nilpotente.
5. Trovare gli elementi nilpotenti e gli elementi idempotenti in un dominio d'integrità unitario.

6. Provare che se A è un anello commutativo unitario, a un elemento invertibile e b nilpotente, allora $a + b$ è invertibile.

7. Trovare gli elementi idempotenti e gli elementi nilpotenti di $\mathbb{Z}_{10}$, $\mathbb{Z}_{12}$ e di $\mathbb{Z}_{10} \times \mathbb{Z}_{12}$.

1. Sia n il minimo intero positivo per cui $a^n = 0$. Tale n esiste per il PBO ed è > 1 poiché $a \neq 0$. Si ha: $a(a^{n-1}) = a^n = 0$ con $a, a^{n-1} \neq 0$, perciò a è zero-divisore.

2. Siccome a è idempotente $a^2 - a = 0 \Leftrightarrow a(a-1) = 0$. Poichè $a \neq 0, a-1 \neq 0$ segue che a è uno zerodivisore.

3. Nell'anello $\mathbb{Z}_4$ $[2]_4$ è diverso da 0, nilpotente e non idempotente. Nell'anello $M_2(\mathbb{R})$ $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ è un elemento non nullo, nilpotente e non idempotente.

4. Nell'anello $\mathbb{Z}_6$ $[3]_6$ è diverso da $0, 1$, idempotente e non nilpotente. Nell'anello $M_2(\mathbb{R})$ $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ è un elemento diverso da $0, 1$, idempotente e non nilpotente.

5. In ogni anello unitario 0 è nilpotente e $0, 1$ sono idempotenti. Se l'anello unitario è anche un dominio di integrità da 1. e 2. segue che non vi sono altri elementi nilpotenti/idempotenti.

6. Essendo b nilpotente $\exists n \in N,\ n > 0\ t.c.\ b^n = 0$. Allora osserviamo che $a^n = a^n - b^n = (a+b)(a^{n-1} + a^{n-2}(-b) + a^{n-3}(-b)^2 + ... + a(-b)^{n-2} + (-b)^{n-1})$. Quindi l'inverso di $a + b$ è $a^{-n}(a^{n-1} + a^{n-2}(-b) + a^{n-3}(-b)^2 + ... + a(-b)^{n-2} + (-b)^{n-1})$.

7. Gli elementi idempotenti di $\mathbb{Z}_{10}$ sono $[0]_{10}, [1]_{10}, [5]_{10}, [6]_{10}$; l'unico elemento nilpotente è $[0]_{10}$, giacché 10 è privo di fattori quadratici.
   Gli elementi idempotenti di $\mathbb{Z}_{12}$ sono $[0]_{12}, [1]_{12}, [4]_{12}, [9]_{12}$ e quelli nilpotenti sono $[0]_{12}, [6]_{12}$.
   In generale, dati A e B anelli $\forall a \in A, \forall b \in B$ si ha: (a, b) è idempotente in $A \times B \Leftrightarrow (a, b)^2 = (a, b) \Leftrightarrow (a^2, b^2) = (a, b) \Leftrightarrow a^2 = a$ e $b^2 = b \Leftrightarrow a$ è idempotente in A e b è idempotente in B.
   In generale, dati A e B anelli $\forall a \in A, \forall b \in B$ si ha: (a, b) è nilpotente in $A \times B \Rightarrow \exists n > 0\ t.c.\ (a, b)^n = (0, 0) \Rightarrow a^n = 0$ e $b^n = 0 \Rightarrow a$ è nilpotente in A, b è nilpotente in B. Vale anche il viceversa: se a è nilpotente in A e b è nilpotente in B allora $\exists n, m > 0\ t.c.\ a^n = 0 = b^m$. Ma quindi (a, b) è nilpotente in $A \times B$ - ad esempio $(a, b)^{n+m} = (0, 0)$. Concludendo: gli elementi idempotenti/nilpotenti di $\mathbb{Z}_{10} \times \mathbb{Z}_{12}$ sono tutte le possibili coppie (a, b) t.c. a è idempotente/nilpotente in $\mathbb{Z}_{10}$ e b è idempotente/nilpotente in $\mathbb{Z}_{12}$.

3. Un anello R si dice *Booleano* se $a^2 = a$ per ogni $a \in R$, i.e. se ogni suo elemento è idempotente. Provare che:

1. per ogni $a \in R$ si ha che $a + a = 0$;

2. R è commutativo.

3. Verificare che sono anelli Booleani:

   (a) $\mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2$;

   (b) per ogni insieme S, $(\mathcal{P}(S), +, \cdot)$, dove $+$ è la differenza simmetrica, $X + Y = X \Delta Y = (X \cup Y) - (X \cap Y)$ per X, Y sottoinsiemi di S, e $\cdot$ è la intersezione.

   (c) per ogni insieme S, $\mathcal{P}_{fin}(S) = \{X \subseteq S \quad | \quad X \text{ finito}\}$ rispetto alla differenza simmetrica e alla intersezione.

4. Verificare che se S è infinito, l'anello $\mathcal{P}_{fin}(S)$ non è unitario.

5. Dare le tabelle per $+$ e $\cdot$ per $\mathcal{P}(S)$ con $S = \{a, b\}$.

1. $(a + a) = (a + a)^2 = a^2 + a^2 + a^2 + a^2 = (a + a) + (a + a) \Rightarrow a + a = 0$;

2. $\forall a, b \in R,\ (a + b) = (a + b)^2 = a^2 + ab + ba + b^2 = (a + b) + ab + ba \Rightarrow ab = -ba = ba$ (per 1.).

3. (a) $\mathbb{Z}_2$ è booleano dato che $[0]_2, [1]_2$ sono idempotenti. $\mathbb{Z}_2 \times \mathbb{Z}_2$ è booleano perché prodotto di due anelli booleani (cfr. ex. 2.7)

   (b) per ogni $X \in \mathcal{P}(S),\ X^2 = X \cdot X = X \cap X = X, .$

   (c) per ogni $X \in \mathcal{P}_{fin}(S),\ X^2 = X \cdot X = X \cap X = X$.

4. Supponiamo per assurdo che $\mathcal{P}_{fin}(S)$ sia unitario. Allora $\exists X \in \mathcal{P}_{fin}(S)$ t.c. $\forall Y \in \mathcal{P}_{fin}(S),\ X \cdot Y = Y \cdot X = Y$. Siccome S ha cardinalità infinita mentre X è finito, possiamo scegliere $z \in S, z \notin X$. Naturalmente anche $Z = X \cup \{z\}$ sta in $\mathcal{P}_{fin}(S)$, ma $Z \cdot X = X \neq Z$.

5. Se $S = \{a, b\}$ allora $\mathcal{P}(S) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.

$+$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a\}$	$\{a\}$	$\emptyset$	$\{a,b\}$	$\{b\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\emptyset$	$\{a\}$
$\{a,b\}$	$\{a,b\}$	$\{b\}$	$\{a\}$	$\emptyset$

$\cdot$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{a\}$	$\emptyset$	$\{a\}$	$\emptyset$	$\{a\}$
$\{b\}$	$\emptyset$	$\emptyset$	$\{b\}$	$\{b\}$
$\{a,b\}$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$

Si noti che $(\mathcal{P}(S), +, \cdot)$ è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

4. Sia A un anello commutativo ed $\mathcal{N}(A)$ l'insieme dei suoi elementi nilpotenti.

1. Provare che $\mathcal{N}(A)$ è un ideale di A detto *nilradicale* o *radicale primo* dell'anello A.

2. Trovare $\mathcal{N}(\mathbb{Z})$ e $\mathcal{N}(\mathbb{Z}_{32})$.

1. cfr. ex. 5.2

2. $\mathbb{Z}$ è un dominio di integrità. Da ex. 2.5 segue che $\mathcal{N}(\mathbb{Z}) = (0)$.
   Invece $\mathcal{N}(\mathbb{Z}_{32}) = ([2]_{32})$.

5. Siano A un anello commutativo ed I un suo ideale; provare che l'insieme $\sqrt{I}$ di tutti gli $a \in A$ tali che $a^n \in I$ per qualche intero positivo n è un ideale di A, detto *radicale* di I.

1. Dare un esempio di un ideale non nullo $I \neq A$ tale che $\sqrt{I} \neq I$ ed un esempio di ideale non nullo $J \neq A$ tale che $\sqrt{J} = J$.

2. Quale relazione si può stabilire tra la nozione di nilradicale di un anello e quella di radicale di un ideale?

Siano $i, j \in \sqrt{I}$. Allora $\exists n, m > 0$ *t.c.* $i^n, j^m \in I$. Consideriamo $(i + j)^{n+m-1} = \sum_{k=0}^{n+m-1} \alpha_k i^k j^{n+m-1-k}$ con $\alpha_k = \binom{n+m-1}{k}$
Visto che se $k < n$ allora $n + m - 1 - k \geq m$ si ha che $(i + j)^{n+m-1} \in I \Rightarrow (i + j) \in \sqrt{I}$.
Inoltre $\forall a \in A$ $ai \in \sqrt{I}$ (infatti $(ai)^n = a^n i^n \in I$). Perciò $\sqrt{I}$ è un ideale.

1. Sia $A = \mathbb{Z}$. Sia $I = (4),\ J = (6)$. Allora $\sqrt{I} = (2) \neq I$ e $\sqrt{J} = (6) = J$.

2. Il nilradicale di un anello altro non è che il radicale dell'ideale nullo.

6. Nell'anello $\mathcal{M}_2(\mathbb{Z}_m)$ con $m > 1$, si consideri il seguente sottoinsieme

$$A_m = \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \ : \ a, b \in \mathbb{Z}_m \right\}.$$

1. Provare che A_m è un sottoanello non commutativo di $\mathcal{M}_2(\mathbb{Z}_m)$ ed è privo di elemento neutro moltiplicativo.

2. Provare che A_m è un ideale sinistro e non è un ideale destro di $\mathcal{M}_2(\mathbb{Z}_m)$.

3. Si consideri l'applicazione $\varphi : A_m \longrightarrow \mathbb{Z}_m$ definita da $\varphi\left(\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}\right) = b$.

   (a) Provare che φ è un omomorfismo.

   (b) Determinare $\mathrm{Im}(\varphi)$ e $\mathrm{Ker}(\varphi)$.

4. Sia $I_m = \left\{ \begin{pmatrix} 0 & 2c \\ 0 & 0 \end{pmatrix} \ : \ c \in \mathbb{Z}_m \right\}$. Provare che I_m è un ideale di A_m.

5. ** Provare che l'anello A_m/I_m è unitario se e solo se m è dispari.

1. $\forall a, b, c, d \in \mathbb{Z}_m$ $\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} - \begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix} = \begin{pmatrix} 0 & a-c \\ 0 & b-d \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}_m)$.
   $\forall a, b, c, d \in \mathbb{Z}_m$ $\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix} = \begin{pmatrix} 0 & ad \\ 0 & bd \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}_m)$.

Pertanto A_m è un sottoanello di $\mathcal{M}_2(\mathbb{Z}_m)$ e non è commutativo: ad esempio $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

Inoltre A_m non è unitario: infatti se $Q = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $\forall P \in A_m$ $PQ = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

2. Per provare che A_m è un ideale sinistro di $\mathcal{M}_2(\mathbb{Z}_m)$, avendo già visto (cfr. ex. 5.1) che ne è un sottogruppo, basta mostrare che $\forall M \in \mathcal{M}_2(\mathbb{Z}_m)$, e $\forall P \in A_m$ $MP \in A_m$. Siano $M = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$, $P = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$ generiche matrici risp. in $\mathcal{M}_2(\mathbb{Z}_m)$ e A_m $(x, y, z, w, a, b \in \mathbb{Z}_m)$. Allora $MP = \begin{pmatrix} 0 & ax + by \\ 0 & az + bw \end{pmatrix} \in A_m$.

   A_m non è un ideale destro: ad esempio $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \notin A_m$.

3. Si consideri l'applicazione $\varphi : A_m \longrightarrow \mathbb{Z}_m$ definita da $\varphi\left(\left(\begin{array}{cc} 0 & a \\ 0 & b \end{array}\right)\right) = b$.

   (a) Per far vedere che ϕ è un omomorfismo bisogna verificare che $\forall P, Q \in A_m$ $\phi(P + Q) = \phi(P) + \phi(Q)$ e $\phi(PQ) = \phi(P)\phi(Q)$. Siano $P = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$, e $Q = \begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix}$ generiche matrici in A_m $(a, b, c, d \in \mathbb{Z}_m)$. Allora $\phi(P + Q) = b + d = \phi(P) + \phi(Q)$ e $\phi(PQ) = bd = \phi(P)\phi(Q)$.

   (b) $\mathrm{Im}(\phi) = \mathbb{Z}_m$, mentre $\ker(\phi) = \left\{ \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}, \ t.c. \ a \in Z_m \right\}$

4. I_m è sia un ideale destro che un ideale sinistro di A_m. Quindi è un ideale di A_m.

5. Sia m dispari.

   Allora $I_m = \ker(\phi)$, (ϕ definito al punto 3.): infatti dato $a \in \mathbb{Z}$ visto che m è dispari, la congruenza $2c \equiv a \mod m$ è sempre risolubile. Quindi, per il teorema fond. di omom. tra anelli, $A_m/I_m \simeq \mathbb{Z}_m$. Siccome $\mathbb{Z}_m$ è un anello unitario, anche A_m/I_m lo è.

   Supponiamo A_m/I_m unitario.

   Allora $\exists P \in A_m$ t.c. P rappresenta l'unità in A_m/I_m. Sia $P = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$, e $Q = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Si deve avere $QP - PQ \in I_m$ e $QP - Q \in I_m$. $QP - PQ = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in I_m \Leftrightarrow \exists c \in \mathbb{Z}_m$ $t.c.$ $2c = b$; $QP - Q = \begin{pmatrix} 0 & b - 1 \\ 0 & 0 \end{pmatrix} \in I_m \Leftrightarrow \exists c' \in \mathbb{Z}_m$ $t.c.$ $2c' = b - 1$ in Z_m. Quindi $\exists c, c' \in \mathbb{Z}_m$ $t.c.$ $1 = 2(c - c')$ in $Z_m \Rightarrow MCD(2, m) = 1$.