Università degli Studi Roma Tre
Corso di Laurea Triennale in Matematica, a.a. 2003/2004
AL2 - algebra 2, gruppi, anelli e campi
Tutorato - Soluzioni
2 dicembre 2003

1. Un ideale I di un anello commutativo ed unitario A si dice *primario* se

$$ab \in I, a \notin I \Longrightarrow \exists n \geq 1 \text{ tale che } b^n \in I.$$

   (a) Verificare che ogni ideale primo di A è primario.

   (b) Provare che un ideale I di A è primario se e solo se ogni zero-divisore di A/I è nilpotente.

   (c) Verificare che l'ideale $8\mathbb{Z}$ di $\mathbb{Z}$ è primario.

   (d) Verificare che l'ideale $6\mathbb{Z}$ di $\mathbb{Z}$ non è primario.

   (e) Dare una caratterizzazione degli ideali primari di $\mathbb{Z}$.

   (a) Sia P ideale primo di A. Allora $ab \in P, a \notin P \Rightarrow b^1 \in P$, quindi P è primario.

   (b) Sia I un ideale primario di A e sia $x + I$ uno zero-divisore di A/I ($x \in A$). Per def. di zero-divisore $x + I \neq 0 + I$ (cioè $x \notin I$) e $\exists y \in A - I$ t.c. $(x + I)(y + I) = 0 + I$ (cioè $xy \in I$). $y \notin I \Rightarrow \exists n \geq 1$ t.c. $x^n \in I$ (per def. di ideale primario) $\Rightarrow (x + I)^n = 0 + I \Rightarrow x + I$ è nilpotente.

   Supponiamo ora che ogni zero-divisore di A/I è nilpotente. Sia $ab \in I, a \notin I$. Quindi $(a+I)(b+I) = 0+I$, da cui $b+I$ o è l'elemento nullo (cioè $b^1 \in I$) o $b+I$ è uno zero-divisore e perciò anche nilpotente per ipotesi: $\exists n \geq 1$ t.c. $b^n \in I$. Si conclude che I è primario.

   (c) Sia $ab \in 8\mathbb{Z}, a \notin 8\mathbb{Z}$. Si ha quindi che $8|ab, 8\nmid a \Rightarrow 2|b$. Perciò $8|b^3 \Rightarrow b^3 \in 8\mathbb{Z}$. Per def. $8\mathbb{Z}$ è primario.

   (d) $2 \cdot 3 \in 6\mathbb{Z},\ 2 \notin 6\mathbb{Z}$, ma $\forall k \geq 1\ \ 3^k \notin 6\mathbb{Z}$.

   (e) Gli ideali primari di $\mathbb{Z}$ sono tutti e soli gli ideali principali della forma (p^k) con p primo.

   Infatti si verifica facilmente che $\forall p \in \mathbb{Z}, p$ primo e $\forall k \in \mathbb{N},\ k \geq 1\ (p^k)$ è un ideale primario. Se poi $I = (m)$ è ideale di $\mathbb{Z}$ e $\exists q, q' \in \mathbb{Z}, q, q' \neq \pm 1, MCD(q, q') = 1$ t.c. $m = qq'$, allora I non è primario: $qq' \in I, q \notin I$ e $\forall k \geq 1\ {q'}^k \notin I$.

2. (a) Sia A un anello commutativo ed unitario dotato di un solo ideale massimale M. Provare che un elemento di A è invertibile se e solo se appartiene a $A - M$.

   (b) Trovare gli ideali massimali di $\mathbb{Z}_5$, di $\mathbb{Z}_9$ e di $\mathbb{Z}_{10}$.

   (c) Determinare per quali interi $m \geq 2$ l'anello $\mathbb{Z}_m$ possiede un solo ideale massimale.

(a) Sia $x \in A$, x invertibile. Allora $x \notin M$ altrimenti $M = A$.

Sia ora $y \in A - M$. Se y non fosse invertibile allora $(y) \subsetneq A$ e quindi per il teorema di Krull $\exists M'$ ideale massimale t.c. $(y) \subseteq M'$. Siccome A ha un solo ideale massimale segue necessariamente che $M = M'$. Perciò $(y) \subseteq M$ che contraddice l'ipotesi.

(b) In generale cerchiamo gli ideali massimali di $\mathbb{Z}_m$ $(m \geq 2)$. Consideriamo l'omomorfismo $\phi : \mathbb{Z} \to \mathbb{Z}_m$ t.c. $\phi(x) = [x]_m$. ϕ è suriettivo e ha nucleo $= m\mathbb{Z}$. Siccome ϕ è suriettivo, ϕ induce una corrispondenza biunivoca, che conserva le inclusioni, tra gli ideali di $\mathbb{Z}_m$ e gli ideali di $\mathbb{Z}$ che contengono $\ker \phi = m\mathbb{Z}$. Siccome la corrispondenza conserva le inclusioni, gli ideali massimali di $\mathbb{Z}_m$ sono tutti i soli gli ideali immagine, tramite ϕ, di ideali massimali in $\mathbb{Z}$ che contengono $m\mathbb{Z}$. Gli ideali massimali in $\mathbb{Z}$ sono tutti e soli della forma (p) con p primo. Inoltre $(m) \subseteq (p) \Leftrightarrow p|m$. In conclusione gli ideali massimali di $\mathbb{Z}_m$ sono gli ideali generati da $[p]_m$ con p primo che divide m.

Nel caso specifico: $\mathbb{Z}_5$ ha solo l'ideale nullo come ideale massimale (e infatti $\mathbb{Z}_5$ è un campo); $\mathbb{Z}_9$ ha solo l'ideale $([3]_9)$ come ideale massimale; $\mathbb{Z}_{10}$ ha due ideali massimali: $([2]_{10})$ e $([5]_{10})$.

(c) Per il punto precedente segue che $\mathbb{Z}_m$ ha un solo ideale massimale sse m ha un solo fattore primo, ovvero $\exists p$ primo, $k \geq 1$ t.c. $m = p^k$.

3. Sia $A = \mathbb{Q}[X]$ l'anello dei polinomi a coefficienti razionali; fissato un numero razionale q, si consideri l'ideale

$$I_q = \{f(X) \in A \mid f(q) = 0\}.$$

(a) Provare che I_q è un ideale massimale di A.

(b) Se q e q' sono due numeri razionali distinti, provare che $I_q \cap I_{q'}$ è un ideale di A che <u>non</u> è un ideale primo.

(a) Proviamo che I_q è un ideale massimale di A in due modi distinti:

i. Consideriamo l'omomorfismo $\phi : \mathbb{Q}[X] \to \mathbb{Q}$ t.c. $\forall f(x) \in \mathbb{Q}[X]$ si ha $\phi(f(x)) = f(q)$.

Si verifica facilmente che ϕ è effettivamente un omomorfismo, è suriettivo e il suo nucleo è proprio I_q. Per il teor. fond. di omom. tra anelli si ha che $\mathbb{Q}[X]/I_q \simeq \mathbb{Q}$. Ma $\mathbb{Q}$ è un campo, perciò I_q è massimale.

ii. I_q certamente contiene l'ideale $J = (X - q) \subsetneq A$. Inoltre $I_q \neq A$ (ad esempio $1 \notin I_q$). $X - q$ è irriducibile in A (è un polinomio di primo grado) e A è un anello a ideali principali $\Rightarrow J$ è un ideale massimale $\Rightarrow I_q = J$ è massimale.

Possibile variante: sfruttando il fatto che A non solo è un dominio a ideali principali, ma è addirittura un dominio euclideo, si può far vedere direttamente che $I_q = J$. Infatti $J \subseteq I_q$ e dato $f(x) \in I_q$ possiamo dividere $f(X)$ per $X - q$: $\exists q(X), r(X) \in A$ con $r(X) = 0$ oppure $deg(r(X)) < deg(X - q) = 1$ t.c. $f(X) = q(X)(X-q)+r(X)$. Questo implica che $r(q) = 0$. Ciò è possibile sse $r(X)$ è il polinomio nullo.

(b) $J = I_q \cap I_{q'}$ è un ideale di A perché intersezione di due ideali. Non è primo: infatti $(X-q)(X-q') \in J$ ma $X-q \notin J$ (visto che $X-q \notin I_{q'}$ dato che $q'-q \neq 0$) e $X-q' \notin J$ (visto che $X-q' \notin I_q$ dato che $q-q' \neq 0$).

4. Sia p un numero primo fissato ed

$$A = \left\{ \begin{pmatrix} a & bp \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}.$$

(a) Verificare che A è un sottoanello di $\mathcal{M}_2(\mathbb{Q})$, commutativo ed unitario.

(b) Provare che A è un campo determinando esplicitamente l'inverso di ogni suo elemento non nullo.

(c) Determinare un isomorfismo esplicito tra A e il campo $\mathbb{Q}[X]/(X^2-p)$.

(a) $\forall a, b, c, d \in \mathbb{Q}$ $\begin{pmatrix} a & bp \\ b & a \end{pmatrix} - \begin{pmatrix} c & dp \\ d & c \end{pmatrix} = \begin{pmatrix} a-c & (b-d)p \\ b-d & a-c \end{pmatrix} \in A$. A quindi è un sgr. di $\mathcal{M}_2(\mathbb{Q})$. Inoltre $\forall a, b, c, d \in \mathbb{Q}$ $\begin{pmatrix} a & bp \\ b & a \end{pmatrix} \begin{pmatrix} c & dp \\ d & c \end{pmatrix}$ $= \begin{pmatrix} c & dp \\ d & c \end{pmatrix} \begin{pmatrix} a & bp \\ b & a \end{pmatrix} = \begin{pmatrix} ac+bdp & (ad+bc)p \\ ad+bc & ac+bdp \end{pmatrix} \in A$. Quindi A è un sottoanello commutativo di $\mathcal{M}_2(\mathbb{Q})$. È anche unitario visto che la matrice identità $\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in A$ $(a = 1, b = 0)$.

(b) Essendo A un sottoanello unitario di $\mathcal{M}_2(\mathbb{Q})$, per verificare che è un campo basta far vedere che $\forall P \in A$, $P \in GL_2(\mathbb{Q})$ e $P^{-1} \in A$.
Sia P una generica matrice di A: $P = \begin{pmatrix} a & bp \\ b & a \end{pmatrix}$, $a, b \in \mathbb{Q}$. $\det(P) = a^2 - b^2 p \neq 0$ (altrimenti $\sqrt{p}$ sarebbe un numero razionale). Quindi $P \in GL_2(\mathbb{Q})$. $P^{-1} = \frac{1}{\det(P)} \begin{pmatrix} a & -bp \\ -b & a \end{pmatrix} \in A$.

(c) Sia $I = (X^2 - p)$. Usando le notazioni al punto precedente, si consideri $\phi : A \to \mathbb{Q}[X]/I$ t.c. $\phi(P) = a + bX + I$. Si verifica facilmente che ϕ è un omomorfismo.
Sia ora $f(X) + I \in \mathbb{Q}[X]/I$. Dividendo $f(X)$ per X^2-p si ottiene un resto $r(X)$ nullo o di grado ≤ 1, cioè $r(x)$ è del tipo $a+bX$ $(a, b \in \mathbb{Q})$. Quindi $\phi(P) = r(X) + I = f(X) + I$, perciò ϕ è suriettivo.
Sia ora $P \in A$ t.c. $\phi(P) = 0 + I$, cioè P è t.c. $a + bX \in I$. Siccome I contiene solo polinomi di grado ≥ 2 oltre al pol. nullo, segue che $a + bX = 0$, ovvero $a, b = 0$, ovvero $P = 0$. Quindi ϕ è iniettivo.

5. Si consideri il seguente sottoinsieme dell'anello $\mathbb{Q}[X]$:

$$A = \{a_0 + a_1 X + \cdots + a_n X^n \mid n \geq 0, a_0 \in \mathbb{Z}, a_i \in \mathbb{Q} \text{ per } i \geq 1\}.$$

(a) Verificare che A è un sottoanello di $\mathbb{Q}[X]$.

(b) Provare che il seguente sottoinsieme di A

$$I = \{b_1 X + \cdots + b_j X^j + \cdots + b_m X^m \mid m \geq 1,\ b_j \in \mathbb{Q} \text{ per} j \geq 1\}$$

è un ideale primo di A.

(c) Descrivere gli elementi dell'ideale generato da X in A.

(d) Provare che I non è un ideale principale. (Sugg. $X \in I$)

(a) Siano $f(X) \in A$, $g(X) \in A$. Quindi $\exists a_0, b_0 \in \mathbb{Z}$ e $a_i, b_j \in Q$ ($1 \leq i \leq n$, $1 \leq j \leq m$, a_n e $b_m \neq 0$) t.c. $f(X) = a_0 + a_1 X + ... + a_n X^n$ e $g(X) = b_0 + b_1 X + ... + b_m X^m$. Allora $f(X) - g(X) = (a_0 - b_0) + (a_1 - b_1)X + ... \in A$ e $f(X)g(X) = a_0 b_0 + (a_0 b_1 + a_1 b_0)X + ... \in A$ (dato che $a_0 - b_0$ e $a_0 b_0 \in \mathbb{Z}$). Quindi A è un sottoanello di $\mathbb{Q}[x]$. Inoltre $1_A = 1_{\mathbb{Q}[X]} = 1$.

(b) $I \subseteq A$ e $I = X\mathbb{Q}[X]$. Quindi I è un ideale primo di $\mathbb{Q}[X]$ (X è un pol.irrid. e $\mathbb{Q}[X]$ è un dominio a ideali principali). Ma allora, dato che A è un sottoanello unitario di $\mathbb{Q}[X]$, I è anche un ideale primo di A.

(c) $XA = \{a_1 X + a_2 X^2 + ... + a_n X^n \text{ con } n \geq 0, a_1 \in \mathbb{Z}, a_i \in \mathbb{Q} \text{ per } i \geq 1\}$.

(d) Supponiamo per assurdo che I è un ideale principale: allora $\exists f(X) \in A$ t.c. $I = f(X)A$. Siccome $X \in I$ allora deve esistere $g(X) \in A$ t.c. $X = g(X)f(X)$. Passando ai gradi: $1 = \deg(X) = \deg(g(X)) + \deg(f(X))$. Dato che $f(X) \in I$ allora $\deg(f(X)) \geq 1$. Quindi $\deg(f(X)) = 1$ e $\deg(g(X)) = 0$, ovvero $g(X) = c \in \mathbb{Z} \Rightarrow f(X) = c^{-1}X$. Consideriamo ora $h(X) = (2c)^{-1}X$. $h(X) \in I$, ma $h(X) \notin f(X)A$ ($h(X)$ si dovrebbe poter scrivere come prodotto di $c^{-1}X$ per una costante in $\mathbb{Z}$, ma $1/2 \notin \mathbb{Z}$). Assurdo.