Università degli Studi Roma Tre
Anno Accademico 2006/2007
AL2 - Algebra 2
Esercitazione 4
Giovedì 30 Novembre 2006

1. Sia $(A, +, \cdot)$ un anello arbitrario. Dimostrare che:
   (a) $0a = 0$ per ogni $a \in A$.
   (b) $-a = (-1)a$ per ogni $a \in A$ (A unitario).
   (c) $(-a)b = -(ab)$ per ogni $a, b \in A$.

   (a) Per ogni $a \in A$, $0a = (0+0)a = 0a + 0a \Rightarrow 0a = 0$.
   (b) Per ogni $a \in A$, $(-1)a + a = (-1)a + 1a = (-1+1)a = 0a = 0 \Rightarrow (-1)a = -a$
   (c) Per ogni $a, b \in A$, $(-a)b + ab = (-a+a)b = 0b = 0 \Rightarrow (-a)b = -(ab)$.

2. Sia $\langle \sqrt[3]{2} \rangle \subseteq \mathbb{C}$ il più piccolo sottoanello di $\mathbb{C}$ che contiene $\sqrt[3]{2}$. Darne una descrizione esplicita.

   $\mathbb{C}$ è un anello commutativo unitario. Per definizione di sottoanello di anello unitario, $\langle \sqrt[3]{2} \rangle$ contiene 1 e quindi tutto $\mathbb{Z}$. Perciò $\mathbb{Z}[\sqrt[3]{2}] := \langle \mathbb{Z} \cup \{\sqrt[3]{2}\} \rangle = \langle \sqrt[3]{2} \rangle$. Sappiamo inoltre che, essendo $\mathbb{C}$ commutativo e unitario, $\mathbb{Z}[\sqrt[3]{2}] = \left\{ \sum_{i=0}^{r} a_i (\sqrt[3]{2})^i \text{ con } a_i \in \mathbb{Z} \text{ per ogni } i = 0, \ldots, r \text{ e } r \geq 0 \right\} = \left\{ a_0 + a_1 \sqrt[3]{2} + a_2 \sqrt[3]{2}^2,\ a_0, a_1, a_2 \in \mathbb{Z} \right\}$.

3. Si consideri $R := \mathbb{Q}[\sqrt{2} + \sqrt{3}]$.
   (a) Dimostrare che $\sqrt{2} + \sqrt{3} \in U(R)$.
   (b) Dimostrare che $R = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

   (a) Sia $\alpha := \sqrt{2}+\sqrt{3}$. $\alpha = \sqrt{2}+\sqrt{3} \Rightarrow \alpha^2 = 2+3-2\sqrt{6} \Rightarrow (\alpha^2-5)^2 = 24$ $\Rightarrow \alpha^4 - 10\alpha^2 + 1 = 0 \Rightarrow 1 = \alpha^2(10-\alpha^2) \Rightarrow \alpha^{-1} = \alpha(10-\alpha^2) \in \mathbb{Q}[\alpha]$.
   (b) $\subseteq$ è ovvia. Dimostriamo ora $\supseteq$, cioé dimostriamo che $\sqrt{2}, \sqrt{3} \in R$: $1 = (\sqrt{3}-\sqrt{2})(\sqrt{3}+\sqrt{2}) \Rightarrow 1/(\sqrt{3}+\sqrt{2}) = \sqrt{3}-\sqrt{2}$. Quindi, per il punto precedente, $\sqrt{3}-\sqrt{2} \in R$. Ma anche $\sqrt{3}+\sqrt{2} \in R$, quindi $\sqrt{3}-\sqrt{2}+\sqrt{3}+\sqrt{2} = 2\sqrt{3} \in R$, cioé $\sqrt{3} \in R$. Analogamente anche $\sqrt{2} \in R$ e l'asserto è dimostrato.

4. Trovare tutti gli endomorfismi (sott.: unitari) dell'anello $\mathbb{R}$.

   Sia $\phi : \mathbb{R} \to \mathbb{R}$ un omomorfismo, $\phi(1) = 1$. Chiaramente, allora, $\phi(n) = n$ per ogni $n \in \mathbb{Z}$ e quindi $\phi(q) = q$ per ogni $q \in \mathbb{Q}$.

   Ora osserviamo che se $a > 0$ allora $\phi(a) > 0$. Infatti $a > 0 \Rightarrow a = (\sqrt{a})^2 \Rightarrow \phi(a) = \phi(\sqrt{a})^2 > 0$.

Sia ora $x \in \mathbb{R} \setminus \mathbb{Q}$. Supponiamo per assurdo che $\phi(x) > x$. Allora $\exists q \in \mathbb{Q}$ t.c. $x < q \leq \phi(x)$. Siccome $q - x > 0$ segue che $\phi(q) - \phi(x) > 0$. Assurdo $(\phi(q) = q)$. Perciò $\phi(x) \leq x$. Analogamente si esclude il caso $\phi(x) < x$. Perciò $\phi(x) = x$. Quindi ϕ è l'identità.

5. Si consideri

$$R := M_2(\mathbb{Q}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in \mathbb{Q} \right\}$$

e se ne determinino tutti gli ideali bilateri.

Gli unici ideali bilateri di R sono $\{0\}$ e R. Infatti: sia I ideale bilatero $\neq \{0\}$. Allora $\exists g \in R$ con $g \neq 0$, $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Q}$. Per semplicità supponiamo $a \neq 0$. Allora $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1/a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Quindi $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in R$.

Analogamente $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1/a & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, quindi anche $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in I$. Ma allora $\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in R$, e perciò $I = R$.

6. Sia $f(X) \in \mathbb{D}[X]$, con $\mathbb{D}$ dominio di integrità. Nei casi seguenti dire se le affermazioni sono vere o false:

   (a) $\mathbb{D} = \mathbb{C}$, $f(X) = 3X^5 + 7X + 1$. $f(X)$ è irriducibile.
   (b) $\mathbb{D} = \mathbb{R}$, $f(X) = X^4 + X + 1$. $f(X)$ è irriducibile.
   (c) Tutti i polinomi di primo grado in $\mathbb{D}[X]$ sono irriducibili.
   (d) $\mathbb{D}$ campo. Tutti i polinomi di primo grado in $\mathbb{D}[X]$ sono irriducibili.
   (e) Se $f(X)$, $\deg(f) \geq 2$, ha una radice in $\mathbb{D}$ allora $f(X)$ è riducibile.
   (f) Se $f(X)$ è riducibile allora $f(X)$ ha una radice in $\mathbb{D}$.
   (g) $\mathbb{D} = \mathbb{Q}$, $f(X) = X^{101} + 2$. f è irriducibile.
   (h) $\mathbb{D} = \mathbb{Q}$, $f(X) = X^3 + 7X + 3$. f è riducibile.
   (i) $\mathbb{D} = \mathbb{Z}$, $f(X) = X^5 + X + 2$. f è riducibile.

   (a) Falsa. Tutti e soli i polinomi irriducibili su $\mathbb{C}$ sono i polinomi di primo grado. Quindi f è riducibile.
   (b) Falsa. Tutti e soli i polinomi irriducibili su $\mathbb{R}$ sono i polinomi di primo grado e i polinomi di secondo grado senza radici reali.
   (c) Falsa. Ad esempio se $\mathbb{D} = \mathbb{Z}$ e $f(X) = 2X$ allora f è riducibile in $\mathbb{Z}$ in quanto $f = 2 \cdot X$.
   (d) Vera. Sia $f(X)$ un polinomio di primo grado. Supponiamo $f(X) = g(X)h(X)$. Allora $\deg(f(X)) = \deg(g(X)) + \deg(h(X))$, quindi o $g(X)$ o $h(X)$ ha grado 0, cioé è una costante non nulla e quindi invertibile per ipotesi.

(e) Vera. Sia α una radice di f. Per il teorema di divisione con resto si ha: $f(X) = (X-\alpha)q(X) + r(X)$ con $q(X), r(X) \in \mathbb{D}[X]$, $\deg(r(X)) < \deg((X-\alpha)) = 1$. Quindi $r(X)$ ha grado 0, i.e. $r(X) = c \in \mathbb{D}$. Inoltre $0 = f(\alpha) = r(\alpha)$, cioé $c = 0$. Perciò $f(X) = (X-\alpha)q(X)$ con $q(X)$ di grado almeno uno (e perciò non invertibile). Quindi $f(X)$ è riducibile.

(f) Falsa. $X^4 + 1$, ad esempio, è riducibile in $\mathbb{R}$ ma non ha radici.

(g) Vera. Basta applicare il criterio di Eisenstein al polinomio a coeff. interi $f(X)$.

(h) Falsa. f, se fosse riducibile, si dovrebbe poter scrivere come prodotto di un polinomio di primo grado ed uno di secondo grado. Perciò f dovrebbe avere una radice in $\mathbb{Q}$. Le radici razionali vanno ricercate tra i divisori di 3: $\pm 1, \pm 3$. Con semplici conti si vede che f non ha radici e che quindi è irriducibile.

(i) Vera. $f(-1) = 0$.

7. Si consideri l'anello $C := \mathbb{R}[X]/I$, dove I è l'ideale (X^2+1). Trovare l'inverso di $X + I$ in C.

$X^2 + 1 + X(-X) = 1 \Rightarrow (X^2 + 1 + I) + (X + I)(-X + I) = 1 + I$. Siccome $X^2 + 1 + I = 0 + I$, in C, si ha che $-X + I$ è l'inverso di $X + I$ in C.

8. Descrivere i nuclei dei seguenti omomorfismi di anelli e dire se sono ideali primi o massimali:

(a) $\phi : \mathbb{R}[X, Y] \to \mathbb{R}$ t.c. $\phi(f(X, Y)) = f(0, 0)$.

(b) $\phi : \mathbb{R}[X] \to \mathbb{C}$ t.c. $\phi(f(X)) = f(2 + i)$.

(a) Chiaramente $(X, Y) \subseteq \ker\phi$. Sia ora $f \in \mathbb{R}[X, Y]$ t.c. $f \in \ker\phi$. $f = \sum_{i=0,j=0}^{i=r,j=s} a_{i,j} X^i Y^j$. Dato che $f(0, 0) = 0$ allora $a_{0,0} = 0$ e perciò $f \in (X, Y)$. Quindi $\ker\phi = (X, Y)$. Dato che ϕ è suriettiva e $\mathbb{R}$ un campo, $\ker\phi$ è un ideale massimale (e primo).

(b) I polinomi reali che hanno come radice $2 + i$ devono necessariamente avere come radice anche $2 - i$. Quindi $\ker\phi = ((X - (2 + i))(X - (2 - i))) = (X^2 - 4X + 5)$. $X^2 - 4X + 5$ è irriducibile e $\mathbb{R}[X]$ è un PID: quindi $(X^2 - 4X + 5)$ è un ideale massimale (e primo).

9. Dire se i seguenti ideali I sono primi o no nell'anello R:

(a) $R := \mathbb{Z}$, $I := (17)$.

(b) $R := \mathbb{Z}[X]$, $I := (14, X)$.

(c) $R := \mathbb{Z}_3[X]$, $I := (X^2 + X + 1)$.

(a) Ogni elemento primo genera un ideale primo. Quindi, essendo 17 primo in $\mathbb{Z}$, I è un ideale primo.

(b) $14 \in I$ ma né 2 né 7 sono in I. Quindi I non è primo.

(c) $X^2 + X + 1 = (X - 1)^2$ in R, quindi $X^2 + X + 1$ è riducibile in R e perciò l'ideale da esso generato non è primo (elemento primo $\Rightarrow$ elemento irriducibile).

10. Sia D dominio di integrità. Provare che $D[X]$ è un PID se, e solo se, D è un campo.

    Il 'se' è già stato dimostrato a lezione: D campo $\Rightarrow D[X]$ è un ED e quindi un PID.

    Per il 'solo se' ragioniamo in questo modo: X è un elemento irriducibile di $D[X]$. Ma allora (X) è un ideale massimale nell'insieme degli ideali principali di $D[X]$. Ma $D[X]$ è PID quindi (X) è un ideale massimale. Perciò $D \cong D[X]/(X)$ è un campo.