Corso di Laurea in Matematica
II compito di ALGEBRA I – 4 maggio 2015
Soluzioni

Esercizio 1. *Siano R un anello e I, J ideali di R; si ponga*

$$L(I,J) = \{x \in R \mid xI \subseteq J\}$$

dove $xI = \{xy \mid y \in I\}$.

1. *Si provi che $L(I,J)$ è un ideale di R,*
2. *Siano $R = \mathbb{Z}$, $1 < n, m \in \mathbb{N}$; si provi che*

$$L(n\mathbb{Z}, m\mathbb{Z}) = \frac{m}{(n,m)}\mathbb{Z}.$$

SOLUZIONE. 1. $L(I,J) \neq \emptyset$, infatti $0_R \in L(I,J)$ poiché $0_R y = 0_R \in J$ per ogni $y \in I$.
Siano $x.x' \in L(I,J)$; allora, per ogni $y \in I$:

$$(x - x')y = xy - x'y \in J$$

dato che $xy \in J$, $x'y \in J$ e J è un ideale. Quindi $x - x' \in L(I,J)$.
Siano $x \in L(I,J)$ e $r \in R$. Allora per ogni $y \in I$, $xy \in J$ e poich'e J è un ideale: $J \ni r(xy) = (rx)y$, provando che $rx \in L(I,J)$. Inoltre, poiché I è un ideale, $ry \in I$ per ogni $y \in I$, e pertanto $J \ni x(ry) = (xr)y$, provando che $xr \in L(I,J)$. Questo completa la dimostrazione che $L(I,J)$ è un ideale di R.

2. Siano n, m come nelle ipotesi e $d = (n,m)$. È chiaro che

$$L(n\mathbb{Z}, m\mathbb{Z}) = \{x \in \mathbb{Z} | x(n\mathbb{Z}) \subseteq m\mathbb{Z}\} = \{x \in \mathbb{Z} | xn \in m\mathbb{Z}\} = \{x \in \mathbb{Z} | m \mid xn\}.$$

Sia $u \in \frac{m}{d}\mathbb{Z}$, cioè $u = \frac{m}{d}z$ con $z \in \mathbb{Z}$; allora $un = \frac{m}{d}nz = m\frac{n}{d}z \in m\mathbb{Z}$ e quindi $u \in L(n\mathbb{Z}, m\mathbb{Z})$.
Viceversa, sia $x \in L(n\mathbb{Z}, m\mathbb{Z})$; allora $m \mid xn$ e quindi $\frac{m}{d} \mid \frac{xn}{d} = \frac{n}{d}x$; poiché $\frac{m}{d}$ e $\frac{n}{d}$ sono coprimi si conclude che $\frac{m}{d}$ divide x ovvero che $x \in \frac{m}{d}\mathbb{Z}$.
Per la doppia inclusione $\frac{m}{d}\mathbb{Z} = L(n\mathbb{Z}, m\mathbb{Z})$.

Esercizio 2. *Sia $A = \{0,1\}^{\mathbb{Z}}$ l'anello delle funzioni da $\mathbb{Z}$ a $\{0,1\} = \mathbb{Z}/2\mathbb{Z}$ e si consideri la funzione $\phi : A \to A$, dove, per ogni $f \in A$, $\phi(f)$ è definita da*

$$\phi(f)(z) = f(2z) \qquad \text{per ogni } \ z \in \mathbb{Z}.$$

1. *Si provi che ϕ è un omomorfismo suriettivo;*
2. *si determini il nucleo $K = \ker(\phi)$ e l'immagine inversa $\phi^{-1}(K)$.*

SOLUZIONE. 1. 1_A è la funzione costante $\underline{1}$; ora, per ogni $z \in \mathbb{Z}$,

$$\phi(\underline{1})(z) = \underline{1}(2z) = 1 = \underline{1}(z)$$

e dunque $\phi(\underline{1}) = \underline{1}$. Siano $f, g \in A$; allora, per ogni $z \in \mathbb{Z}$,

$$\phi(f)(z) + \phi(g)(z) = f(2z) + g(2z) = (f+g)(2z) = \phi(f+g)(z)$$

e dunque $\phi(f) + \phi(g) = \phi(f+g)$. Inoltre

$$(\phi(f)\phi(g))(z) = \phi(f)(z)\phi(g)(z) = f(2z)g(2z) = (fg)(2z) = \phi(fg)(z)$$

e dunque $\phi(f)\phi(g) = \phi(fg)$. Pertanto, ϕ è un omomorfismo.
Sia $g \in A$; definiamo $f \in A$ ponendo, per ogni $z \in \mathbb{Z}$

$$f(z) = \begin{cases} g(z/2) & \text{se } z \in 2\mathbb{Z} \\ 0 & \text{se } z \notin 2\mathbb{Z} \end{cases}$$

Allora, per ogni $z \in \mathbb{Z}$

$$\phi(f)(z) = f(2z) = g(\frac{2z}{2}) = g(z)$$

e dunque $\phi(f) = g$, provando che ϕ è suriettivo.

2. 0_A è la funzione costante $\underline{0}$; quindi, posto $K = \ker(\phi)$,

$$K = \{f \in A \mid \phi(f) = \overline{0}\} = \{f \in A \mid f(2z) = 0 \forall z \in \mathbb{Z}\} = \{f \in A \mid f(2\mathbb{Z}) = 0\}.$$

Sia $f \in \phi^{-1}(K)$; allora $\phi(f) \in K$, cioè per ogni $z \in \mathbb{Z}$,

$$0 = \phi(f)(2z) = f(4z)$$

Quindi $\phi^{-1}(K) = \{f \in A \mid f(4\mathbb{Z}) = 0\}$.

Esercizio 3. *Sia $\mathbb{Z}[i]$ l'anello degli interi di Gauss. Si dica se l'anello quoziente $E = \mathbb{Z}[i]/(13)$ è un campo; si dica quindi quali sono gli ideali di E.*

SOLUZIONE. Per $z = a+ib \in \mathbb{C}$ ricordo la definizione di *norma di z*, $N(z) = a^2+b^2$, e che un elemento $u \in \mathbb{Z}[i]$ è invertibile se e solo se $N(u) = 1$, che equivale a $u \in \{1, -1, i, -i\}$. Ora $13 = (2+3i)(2-3i)$; poiché $N(2+3i) = N(2-3i) = 13 \neq 1$, nessuno dei due fattori è invertibile, dunque 13 non è un elemento irriducibile di $\mathbb{Z}[i]$, pertanto, poiché $\mathbb{Z}[i]$ è un P.I.D., (13) non è un ideale massimale e conseguentemente $\mathbb{Z}[i]/(13)$ non è un campo.
Osserviamo poi che $2+3i$ e $2-3i$ sono irriducibili; infatti se $2+3i = xy$ con $x, y \in \mathbb{Z}[i]$, allora $13 = N(2+3i) = N(x)N(y)$ da cui segue che $N(x) = 1$, cioè x invertibile, oppure $N(y) = 1$ e y invertibile; lo stesso argomento vale per $2-3i$. Dunque $13 = (2+3i)(2-3i)$ è una fattorizzazione in irriducibili di 13; inoltre, come si verifica facilmente $2+3i$ e $2-3i$ non sono associati. Dal Teorema di corrispondenza e dal fatto che $\mathbb{Z}[i]$ è a ideali principali segue che gli ideali dell'anello quoziente $E = \mathbb{Z}[i]/(13)$ sono

$$(13)/(13) = \{0_E\}, \quad (2+3i)/(13), \quad (2-3i)/(13), \quad E.$$

Esercizio 4. *Sia p un numero primo positivo; in $(\mathbb{Z}/p\mathbb{Z})[x]$ si consideri*

$$f_p = x^p - \overline{11}x^{p-1} + \overline{11}x - \overline{11}$$

1. *Si provi che se $p \neq 3$ allora f_p ha una radice in $\mathbb{Z}/p\mathbb{Z}$.*
2. *Posto $p = 5$ si decomponga f_5 come prodotto di irriducibili in $(\mathbb{Z}/5\mathbb{Z})[x]$.*
3. *Posto $p = 3$ sia $E = (\mathbb{Z}/p\mathbb{Z})[x]/(f_3)$; si dica se E è un campo e qual è il suo ordine; in E si calcoli quindi $(x + (f_3))^{-1}$.*

SOLUZIONE. 1. Per $p = 2$ si ha

$$f_2 = x^2 - x + x - \bar{1} = x^2 - \bar{1} = (x - \bar{1})^2$$

quindi in particolare $f_2(1) = \bar{0}$.
Se $p = 11$, $f_{11} = x^{11}$ e $f_{11}(\bar{0}) = \bar{0}$.
Sia $p \neq 2, 3, 11$. Se $\bar{0} \neq \bar{a} \in \mathbb{Z}/p\mathbb{Z}$ allora, per il Teorema di Fermat,

$$f_p(\bar{a}) = \bar{a}^p - \overline{11}\bar{a}^{p-1} + \overline{11}\bar{a} - \overline{11} = \bar{a} - \overline{11} + \overline{11}\bar{a} - \overline{11} = \overline{12}\bar{a} - \overline{22}.$$

Poiché $p \neq 2, 3$, $\overline{12} \neq \bar{0}$ è invertibile e $f_p(\overline{22}/\overline{12}) = \bar{0}$.

attenzione: Scrivere che, per Fermat, $x^p - \overline{11}x^{p-1} + \overline{11}x - \overline{11} = x - \overline{11} + \overline{11}x - \overline{11}$ è un errore (l'ho valutato al minimo, ma è un errore); i due polinomi sono diversi, sono le rispettive funzioni di sostituzione, con dominio ridotto a $\mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$ ad essere uguali.

2. Sia $p = 5$, quindi $f_5 = x^5 - \overline{11}x^4 + \overline{11}x - \overline{11} = x^5 - x^4 + x - \bar{1} = (x - \bar{1})(x^4 + \bar{1})$. Ora, in $\mathbb{Z}/5\mathbb{Z}$,

$$x^4 + \bar{1} = x^4 - \bar{4} = (x^2 + \bar{2})(x^2 - \bar{2}).$$

Poiché i polinomi $x^2 + \bar{2}$ e $x^2 - \bar{2}$ sono irriducibili in $(\mathbb{Z}/5\mathbb{Z})[x]$ (non hanno radici in $\mathbb{Z}/5\mathbb{Z}$), si conclude che

$$f_5 = (x - \bar{1})(x^2 - \bar{2})(x^2 + \bar{2})$$

è una fattorizzazione in irriducibili di f_5 in $(\mathbb{Z}/5\mathbb{Z})[x]$.

3. Sia $p = 3$ e quindi $f_3 = x^3 - \overline{11}x^2 + \overline{11}x - \overline{11} = x^3 + x^2 - x + \bar{1}$. Si ha $f_3(\bar{0}) = \bar{1}$, $f_3(\bar{1}) = \bar{2}$, $f_3(\bar{2}) = \bar{2}$, quindi f_3 non ha radici in $\mathbb{Z}/3\mathbb{Z}$; poiché $\mathbb{Z}/3\mathbb{Z}$ è un campo, f_3 non ha fattori di grado 1 in $(\mathbb{Z}/3\mathbb{Z})[x]$ e dunque, poichè ha grado 3, f_3 è irriducibile in $(\mathbb{Z}/3\mathbb{Z})[x]$. Poiché $(\mathbb{Z}/3\mathbb{Z})[x]$ è un P.I.D., $E = (\mathbb{Z}/3\mathbb{Z})[x]/(f_3)$ è un campo.

Dai risultati noti sappiamo che ogni elemento dell'anello quoziente E si scrive in modo unico nella forma

$$a_0 + a_1x + a_2x^2 + (f_3)$$

con $a_0, a_1, a_2 \in \mathbb{Z}/3\mathbb{Z}$. Per ognuno dei coefficienti a_0, a_1, a_2 si hanno tre scelte, e quindi $|E| = 3^3 = 27$.

Per quanto appena ricordato, esistono $a_0, a_1, a_2 \in \mathbb{Z}/3\mathbb{Z}$ tali che

$$1_E = \bar{1} + (f_3) = (x + (f_3))(a_0 + a_1x + a_2x^2 + (f_3)). \tag{1}$$

Inoltre, in E, $0_E = (f_3) = x^3 + x^2 - x + \bar{1} + (f_3)$ e quindi $x^3 + (f_3) = -x^2 + x + \bar{2} + (f_3)$. Da (1) si ricava dunque

$$\bar{1} + (f_3) = a_0 x + a_1 x^2 + a_2 x^3 + (f_3) = 2a_2 + (a_0 + a_2)x + (a_1 - a_2)x^2 + (f_3),$$

quindi

$$\begin{cases} 2a_2 = \bar{1} \\ a_0 + a_2 = \bar{0} \\ a_1 - a_2 = \bar{0} \end{cases} \quad \Leftrightarrow \quad \begin{cases} a_2 = \bar{2} \\ a_0 = \bar{1} \\ a_1 = \bar{2} \end{cases}$$

Pertanto $(x + (f_3))^{-1} = \bar{1} + \bar{2}x + \bar{2}x^2 + (f_3) = \bar{1} - x - x^2 + (f_3)$.

attenzione: Il Criterio di Eisenstein funziona per polinomi in $\mathbb{Z}[x]$; applicarlo a polinomi a coefficienti su altri anelli (in particolare campi) è cosa senza senso (in effetti una sciocchezza).

Esercizio 5. *Sia A un dominio ad ideali principali e $\phi : A \to A$ un omomorfismo suriettivo; si provi che ϕ è un isomorfismo.*

Soluzione. Siano A e ϕ come nel testo e supponiamo, per assurdo, che ϕ non sia un isomorfismo. Allora ϕ non è iniettivo e dunque, dato che A è un dominio a ideali principali, $\ker(\phi) = (a)$ con $0_A \neq a \in A$. Per il teorema di omomorfismo si ha

$$A/(a) \simeq Im(\phi) = A.$$

Quindi $A/(a)$ è in particolare un dominio d'integrità e dunque a è un elemento primo di A. Poiché A è un P.I.D., a è irriducibile e dunque $A \simeq A/(a)$ è un campo. Ma allora $a \neq 0_A$ è invertibile il che comporta l'assurdo $\ker(\phi) = (a) = A$.