ALGEBRA I: SOLUZIONI SESTA ESERCITAZIONE
12 maggio 2011

Esercizio 1. Mostrare che i seguenti ideali non sono principali (dove $\Bbbk$ è un campo):

$$(2,x) \subset \mathbb{Z}[x], \qquad (x,y) \subset \Bbbk[x,y].$$

Soluzione. Supponiamo che $(2,x) \subset \mathbb{Z}[x]$ sia un ideale principale e sia $p(x) \in \mathbb{Z}[x]$ un generatore $(2,x)$. Il fatto che $p(x)$ divide 2 implica che $p(x)$ è costante ed uguale a 1 o 2 (a meno del segno), d'altra parte 2 non divide x in $\mathbb{Z}[x]$, pertanto $p(x) = 1 = \mathrm{MCD}(2,x)$. Ma questo è assurdo perché

$$(2,x) = \{p(x) \in \mathbb{Z}[x] \ : \ p(0) \text{ è pari}\} :$$

pertanto $1 \notin (2,x)$, vale a dire $(2,x)$ non è un ideale principale.

Similmente si mostra che $(x,y) \subset \Bbbk[x,y]$ non è principale: anche in questo caso si mostra che se $p(x)$ fosse un generatore di (x,y) allora dovrebbe essere $p(x) = \mathrm{MCD}(x,y) = 1$. D'altra parte

$$(x,y) = \{p(x,y) \in \Bbbk[x,y] \ : \ p(0,0) = 0\},$$

Dunque $1 \notin (x,y)$ e (x,y) non è un ideale principale.

Osservazione. Questi esempi mostrano che in un dominio a fattorizzazione unica non necessariamente il massimo comune divisore di due elementi ammette un'identità di Bézout. Se infatti il massimo comune divisore d di due elementi a, b ammette un'identità di Bézout, allora esso appartiene all'ideale (a,b) e di conseguenza $(a,b) = (d)$ è un ideale principale. Pertanto l'esistenza di un identità di Bézout per il massimo comune divisore di a, b equivale al fatto che l'ideale (a,b) è principale. Pertanto l'esistenza dell'identità di Bézout (per ogni coppia di elementi) caratterizza i domini a ideali principali all'interno dei domini a fattorizzazione unica.

Esercizio 2. Sia $I \subset \mathbb{Z}$ un ideale. Mostare che I è primo se e solo se $I = (p)$ per qualche numero primo $p \in \mathbb{Z}$.

Soluzione. Supponiamo che I è un ideale primo: poiché in $\mathbb{Z}$ ogni ideale è principale, possiamo scrivere $I = (n)$ per qualche $n \in \mathbb{Z}$. Mostriamo che (a meno del segno) n è un numero primo. Siano $a, b \in \mathbb{Z}$ tali che n divide ab: dunque $ab \in I$. Dalla definizione di ideale primo, otteniamo che a oppure b appartengono a I: pertanto n divide almeno uno tra a e b e dunque è un numero primo.

Supponiamo viceversa che p è un numero primo e vediamo che (p) è un ideale primo. Siano $a, b \in \mathbb{Z}$ tali che $ab \in I$: dunque n divide ab. Dalla definizione di numero primo, otteniamo che n divide almeno uno tra a e b: dunque a oppure b appartengono a I, vale a dire I è un ideale primo.

Esercizio 3. Sia $\phi : A \to B$ un omomorfismo di anelli.

i) Mostrare che se $P \subset B$ è un ideale primo, allora $\phi^{-1}(P) \subset A$ è un ideale primo.

ii) Mostrare con un controesempio che se $P \subset B$ è un ideale massimale, allora non necessariamente $\phi^{-1}(P) \subset A$ è un ideale massimale.

Soluzione. i) Siano $a, b \in A$ tali che $ab \in \phi^{-1}(P)$: ciò vuol dire che $\phi(ab) \in P$. D'altra parte $\phi(ab) = \phi(a)\phi(b)$ e, siccome P è primo, otteniamo che $\phi(a) \in P$ oppure $\phi(b) \in P$: equivalentemente, abbiamo ottenuto che $a \in \phi^{-1}(P)$ oppure $b \in \phi^{-1}(P)$, vale a dire $\phi^{-1}(P)$ è un ideale primo.

ii) Sia $A = \mathbb{Z}[x]$ e sia $B = \mathbb{Q}[x]$, sia $\phi : \mathbb{Z}[x] \to \mathbb{Q}[x]$ l'immersione naturale. Consideriamo l'ideale $P = (x) \subset \mathbb{Q}[x]$: allora P è massimale perché $\mathbb{Q}[x]/P \simeq \mathbb{Q}$ è un campo. D'altra parte $\phi^{-1}(P) = P \cap \mathbb{Z}[x]$ è l'ideale generato da x in $\mathbb{Z}[x]$: pertanto $\mathbb{Z}[x]/\phi^{-1}(P) \simeq \mathbb{Z}$ non è un campo e $\phi^{-1}(P)$ non è massimale (ad esempio $(x) \subsetneq (2,x) \subsetneq \mathbb{Z}[x]$).

Esercizio 4. (*Teorema cinese del resto*) Siano r e s due numeri interi coprimi. Mostrare che la proiezione

$$\phi : \mathbb{Z} \longrightarrow \mathbb{Z}/(r) \times \mathbb{Z}/(s).$$

induce un isomorfismo di anelli $\mathbb{Z}/(rs) \simeq \mathbb{Z}/(r) \times \mathbb{Z}/(s)$.

Soluzione. Sia $n \in \ker \phi$ un elemento del nucleo di ϕ: allora $n \in (r) \cap (s)$ e n è un multiplo comune di r e s, dunque n è un multiplo del minimo comune multiplo di r e s. D'altra parte, poiché r e s sono coprimi, il minimo comune multiplo di r e s coincide con il prodotto rs, dunque abbiamo mostrato che rs divide n, vale a dire $\ker \phi \subset (rs)$. D'altra parte $rs \in \ker \phi$, dunque $\ker \phi = (rs)$ e dal teorema fondamentale di omomorfismo per anelli otteniamo che ϕ induce un isomorfismo di $\mathbb{Z}/(rs)$ con un sottoanello di $A \subset \mathbb{Z}/(r) \times \mathbb{Z}/(s)$. D'altra parte $\mathbb{Z}/(rs)$ e $\mathbb{Z}/(r) \times \mathbb{Z}/(s)$ sono entrambi insiemi finiti di cardinalità rs, pertanto $A = \mathbb{Z}/(r) \times \mathbb{Z}/(s)$ ed abbiamo ottenuto l'isomorfismo desiderato.

Esercizio 5. (*Teorema cinese del resto in anelli arbitrari*) Sia A un anello e siano $I, J \subset A$ due ideali (bilateri) tali che $I + J = A$. Mostrare che la proiezione

$$\phi : A \simeq A/I \times A/J.$$

induce un isomorfismo di anelli $A/I \cap J \longrightarrow A/I \times A/J$.

Soluzione. Si osservi prima di tutto che $I \cap J$ coincide con il nucleo di ϕ: pertanto per il teorema fondamentale di omomorfismo ϕ induce un'immersione $A/I \cap J \longrightarrow A/I \times A/J$ e l'isomorfismo cercato segue se mostriamo che ϕ è suriettiva.

Sia $(a + I, b + J) \in A/I \times A/J$. Poiché $I + J = A$, possiamo scrivere $a = i + j$ e $b = i' + j'$ con $i, i' \in I$ e $j, j' \in J$. Consideriamo l'immagine dell'elemento $i' + j \in A$:

$$\phi(i' + j) = (i' + j + (i - i') + I, i' + j + (j' - j) + J) = (i + j + I, i' + j' + J) = (a + I, b + J).$$

Pertanto ϕ è suriettiva e segue l'isomorfismo $A/I \cap J \simeq A/I \times A/J$.

Definizione. Un anello si dice *locale* se possiede un unico ideale massimale.

Esercizio 6. Sia $p \in \mathbb{Z}$ un numero primo e si consideri il sottoinsieme di $\mathbb{Q}$ definito da

$$\mathbb{Z}_{(p)} = \{a/b \ : \ a, b \in \mathbb{Z} \ \text{ e } \ p \text{ non divide } b\} :$$

tale sottoinsieme è detto la *localizzazione* di $\mathbb{Z}$ in p.

i) Mostare che $\mathbb{Z}_{(p)}$ è un sottoanello di $\mathbb{Q}$.

ii) Mostrare che il sottoinsieme $I = \left\{a/b \in \mathbb{Z}_{(p)} \ : \ p \text{ divide } a\right\}$ è un ideale di $\mathbb{Z}_{(p)}$.

iii) Mostrare che l'insieme degli invertibili di $\mathbb{Z}_{(p)}$ coincide con $\mathbb{Z}_{(p)} \smallsetminus I$.

iv) Mostrare che I è l'unico ideale massimale di $\mathbb{Z}_{(p)}$.

Soluzione. i) E' immediato verificare che $0, 1 \in \mathbb{Z}_{(p)}$, pertanto è sufficiente verificare che $\mathbb{Z}_{(p)}$ è chiuso rispetto alle operazioni di somma, sottrazione e prodotto definite in $\mathbb{Q}$. Siano $a/b, c/d \in \mathbb{Z}_{(p)}$, allora

$$\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd} \qquad \text{e} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} :$$

pertanto per concludere è sufficiente mostrare che p non divide bd. Ma questo segue dal fatto che p è un numero primo: se p dividesse il prodotto bd, allora p dividerebbe almeno uno tra b e d, contraddicendo l'ipotesi $a/b, c/d \in \mathbb{Z}_{(p)}$.

ii) E' sufficiente mostrare che I è chiuso rispetto alle operazioni di somma e sottrazione e rispetto al prodotto per un elemento di $\mathbb{Z}_{(p)}$. Siano $a/b, c/d \in I$, allora $a/b \pm c/d = (ad \pm bc)/cd$: pertanto per mostrare che $a/b \pm c/d \in I$ è sufficiente mostrare che p divide il numeratore $ad \pm bc$, che segue immediatamente dal fatto che p divide entrambi a e c. Siano ora $a/b \in I$ e $c/d \in \mathbb{Z}_{(p)}$ a mostriamo che il loro prodotto è in I. Poiché divide a, p divide anche ac; d'altra parte p non divide bd poiché esso non divide né b né d: pertanto $ac/bd \in I$.

iii) Sia $a/b \in \mathbb{Z}_{(p)}$ un elemento invertibile. Poiché $\mathbb{Z}_{(p)}$ è un sottoanello di $\mathbb{Q}$, ciò vuol dire che $b/a \in \mathbb{Z}_{(p)}$, vale a dire che p non divide a: pertanto $a/b \in \mathbb{Z}_{(p)} \smallsetminus I$. Supponiamo viceversa che $a/b \in \mathbb{Z}_{(p)} \smallsetminus I$: allora p non divide a, vale a dire $b/a \in \mathbb{Z}_{(p)}$ e a/b è invertibile.

iv) Sia J un ideale di $\mathbb{Z}_{(p)}$ e supponiamo che $J \not\subset I$. Allora $J \cap (\mathbb{Z}_{(p)} \smallsetminus I) \neq \varnothing$, vale a dire J contiene un elemento invertibile e $J = \mathbb{Z}_{(p)}$. Pertanto ogni ideale diverso da $\mathbb{Z}_{(p)}$ è contenuto in I, vale a dire I è l'unico ideale massimale di $\mathbb{Z}_{(p)}$.

Esercizio 7. Sia A un dominio d'integrità con campo dei quozienti Q e sia $P \subset A$ un ideale primo. Si consideri il sottoinsieme di Q definito da

$$A_P = \{a/b \ : \ a, b \in A \ \text{ e } \ b \notin P\} :$$

tale sottoinsieme è detto la *localizzazione* di A in P.

i) Mostare che A_P è un sottoanello di Q.

ii) Mostrare che il sottoinsieme $I = \{a/b \in A_P \ : \ a \in P\}$ è un ideale di A_P.

iii) Mostrare che l'insieme degli invertibili di A_P coincide con $A \smallsetminus I$.

iv) Mostrare che I è l'unico ideale massimale di A_P.

Soluzione. i) E' immediato verificare che $0, 1 \in A_P$, pertanto è sufficiente verificare che A_P è chiuso rispetto alle operazioni di somma, sottrazione e prodotto definite in Q. Siano $a/b, c/d \in A_P$, allora

$$\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd} \qquad \text{e} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} :$$

pertanto per concludere è sufficiente mostrare che $bd \notin P$. Ma questo segue dal fatto che P è un ideale primo: se fosse $bd \in P$, allora sarebbe anche $b \in P$ o $d \in P$, contraddicendo l'ipotesi $a/b, c/d \in A_P$.

ii) E' sufficiente mostrare che I è chiuso rispetto alle operazioni di somma e sottrazione e rispetto al prodotto per un elemento di A_P. Siano $a/b, c/d \in I$, allora $a/b \pm c/d = (ad + \pm bc)/cd$: pertanto per mostrare $a/b \pm c/d \in I$ è sufficiente mostrare che $ad \pm bc \in P$. Ma questo segue immediatamente dal fatto che segue P è un ideale e che $a, c \in P$. Siano ora $a/b \in I$ e $c/d \in A_P$ e mostriamo che $ac/bd \in I$: infatti $ac \in P$ poiché $a \in P$, mentre $bd \notin P$ poiché P è primo e $b, d \notin P$.

iii) Sia $a/b \in A_P$ un elemento invertibile. Poiché A_P è un sottoanello di Q, ciò vuol dire che $b/a \in A_P$, vale a dire che $a \notin P$: pertanto $a/b \in A_P \smallsetminus I$. Supponiamo viceversa che $a/b \in A_P \smallsetminus I$: allora $a \notin P$, vale a dire $b/a \in A_P$ e a/b è invertibile.

iv) Sia J un ideale di A_P e supponiamo che $J \not\subset I$. Allora $J \cap (A_P \smallsetminus I) \neq \varnothing$, vale a dire J contiene un elemento invertibile e $J = A_P$. Pertanto ogni ideale diverso da A_P è contenuto in I, vale a dire I è l'unico ideale massimale di A_P.