Corso di Laurea in Matematica
II Compito di ALGEBRA I
2 maggio 2012

Esercizio 1. (8 punti) Siano

$$A := \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{Z}_{11} \right\} \qquad \text{e} \qquad I := \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{Z}_{11} \right\}$$

1. Si provi che A è un anello, rispetto alle usuali operazioni di somma e prodotto di matrici, e che I è un ideale di A.
2. Si determinino i divisori dello zero e gli invertibili dell'anello quoziente A/I.

Esercizio 2. (10 punti) Sia

$$I = \{a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x] \ : \ a_0 \in 18\mathbb{Z}\} \ .$$

1. Si provi che I è un ideale di $\mathbb{Z}[x]$.
2. Si stabilisca se I è primo e/o principale.
3. Determinare gli ideali massimali di $\mathbb{Z}[x]$ che contengono I.
4. Determinare la caratteristica dell'anello quoziente $\mathbb{Z}[x]/I$.

Esercizio 3. (10 punti) Si provi che $\mathbb{Z}[\sqrt{-14}]$ non è un dominio a fattorizzazione unica. Si trovi un elemento irriducibile, ma non primo, di $\mathbb{Z}[\sqrt{-14}]$. Si determini una coppia di elementi di $\mathbb{Z}[\sqrt{-14}]$ che non ammette massimo comun divisore in $\mathbb{Z}[\sqrt{-14}]$.

Esercizio 4. (4 punti) Siano $f = x^4 - 2x^3 + 2x^2 - 2x + 1$, $g = x^3 - x^2 - x + 1$ e sia $I = (f, g)$ l'ideale generato da f e g in $\mathbb{Q}[x]$. Si trovi un elemento nilpotente non nullo dell'anello quoziente $\mathbb{Q}[x]/I$.

Esercizio 1: (1) $A=\left\{\begin{pmatrix} a & b \\ 0 & c\end{pmatrix} \,\middle|\, a,b,c\in\mathbb{Z}_{11}\right\}$ è un sottoanello di $M_2(\mathbb{Z}_{11})$.

Infatti:

- $1_{M_2(\mathbb{Z}_{11})}=\begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix}\in A$.
- Se $\begin{pmatrix} a & b \\ 0 & c\end{pmatrix},\begin{pmatrix} d & e \\ 0 & f\end{pmatrix}\in A$, $\begin{pmatrix} a & b \\ 0 & c\end{pmatrix}-\begin{pmatrix} d & e \\ 0 & f\end{pmatrix}=\begin{pmatrix} a-d & b-e \\ 0 & c-f\end{pmatrix}\in A$

e $\begin{pmatrix} a & b \\ 0 & c\end{pmatrix}\begin{pmatrix} d & e \\ 0 & f\end{pmatrix}=\begin{pmatrix} ad & ae+bf \\ 0 & cf\end{pmatrix}\in A$.

Oss: A non è commutativo: $\begin{pmatrix} 1 & 1 \\ 0 & 0\end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 1\end{pmatrix}\neq\begin{pmatrix} 0 & 1 \\ 0 & 1\end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0\end{pmatrix}$

I è un ideale di A: usando la definizione (oppure: vedi punto (2))

- $\begin{pmatrix} 0 & 0 \\ 0 & 0\end{pmatrix}\in I$; quindi $I\neq\emptyset$.
- Se $\begin{pmatrix} 0 & b \\ 0 & 0\end{pmatrix},\begin{pmatrix} 0 & e \\ 0 & 0\end{pmatrix}\in I$, allora $\begin{pmatrix} 0 & b \\ 0 & 0\end{pmatrix}-\begin{pmatrix} 0 & e \\ 0 & 0\end{pmatrix}=\begin{pmatrix} 0 & b-e \\ 0 & 0\end{pmatrix}\in I$
- Se $\begin{pmatrix} 0 & b \\ 0 & 0\end{pmatrix}\in I$, $\begin{pmatrix} d & e \\ 0 & f\end{pmatrix}\in A$, allora $\begin{pmatrix} 0 & b \\ 0 & 0\end{pmatrix}\begin{pmatrix} d & e \\ 0 & f\end{pmatrix}=\begin{pmatrix} 0 & bf \\ 0 & 0\end{pmatrix}\in I$

e $\begin{pmatrix} d & e \\ 0 & f\end{pmatrix}\begin{pmatrix} 0 & b \\ 0 & 0\end{pmatrix}=\begin{pmatrix} 0 & db \\ 0 & 0\end{pmatrix}\in I$.

---

(2) $\phi: A\to\mathbb{Z}_{11}\times\mathbb{Z}_{11}$, definita da, per $\begin{pmatrix} a & b \\ 0 & c\end{pmatrix}\in A$,

$\phi\left(\begin{pmatrix} a & b \\ 0 & c\end{pmatrix}\right)=(a,c)$ è un omomorfismo suriettivo.

Infatti: (a) $\forall\begin{pmatrix} a & b \\ 0 & c\end{pmatrix},\begin{pmatrix} d & e \\ 0 & f\end{pmatrix}\in A$,

- $\phi\left(\begin{pmatrix} a & b \\ 0 & c\end{pmatrix}+\begin{pmatrix} d & e \\ 0 & f\end{pmatrix}\right)=\phi\left(\begin{pmatrix} a+d & b+e \\ 0 & c+f\end{pmatrix}\right)=(a+d,c+f)=\phi\left(\begin{pmatrix} a & b \\ 0 & c\end{pmatrix}\right)+\phi\left(\begin{pmatrix} d & e \\ 0 & f\end{pmatrix}\right)$
- $\phi\left(\begin{pmatrix} a & b \\ 0 & c\end{pmatrix}\begin{pmatrix} d & e \\ 0 & f\end{pmatrix}\right)=\phi\left(\begin{pmatrix} ad & ae+bf \\ 0 & cf\end{pmatrix}\right)=(ad,cf)=(a,c)(d,f)=\phi\left(\begin{pmatrix} a & b \\ 0 & c\end{pmatrix}\right)\cdot\phi\left(\begin{pmatrix} d & e \\ 0 & f\end{pmatrix}\right)$.

(b) $\phi\left(\begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix}\right)=(1,1)=1_{\mathbb{Z}_{11}\times\mathbb{Z}_{11}}$

Inoltre, per ogni $(a,c)\in\mathbb{Z}_{11}\times\mathbb{Z}_{11}$, $(a,c)=\phi\left(\begin{pmatrix} a & 0 \\ 0 & c\end{pmatrix}\right)$, con $\begin{pmatrix} a & 0 \\ 0 & c\end{pmatrix}\in A$.

Si ha

$\operatorname{Ker}\phi=\left\{\begin{pmatrix} a & b \\ 0 & c\end{pmatrix} \,\middle|\, a=0=c\right\}=I$ (questo prova, senza bisogno della verifica del punto (1), che I è un ideale di A).

Per il teorema di omomorfismo:

$\bar\phi:\dfrac{A}{I}\to\mathbb{Z}_{11}\times\mathbb{Z}_{11}$ def. da $\bar\phi\left(\begin{pmatrix} a & b \\ 0 & c\end{pmatrix}+I\right)=(a,c)$

è un isomorfismo.

Segue: $U(A/I) = \Phi^{-1}(U(\mathbb{Z}_{11}\times\mathbb{Z}_{11})) = \Phi^{-1}\left(\left\{(a,c) \;\middle|\; \begin{matrix} a,c\in\mathbb{Z}_{11} \\ a\neq 0 \\ c \neq 0\end{matrix}\right\}\right)$

$= \left\{\begin{pmatrix} a & b \\ 0 & c\end{pmatrix}+I \;\middle|\; \begin{matrix} a,b,c\in\mathbb{Z}_{11} \\ a\neq 0,\ c\neq 0\end{matrix}\right\} = \left\{\begin{pmatrix} a & 0 \\ 0 & c\end{pmatrix}+I \;\middle|\; \begin{matrix} a,c\in\mathbb{Z}_{11} \\ a\neq 0,\ c\neq 0\end{matrix}\right\}$

Analogamente, l'insieme dei divisori dello zero di A/I

è $\left\{\begin{pmatrix} a & b \\ 0 & c\end{pmatrix}+I \;\middle|\; \begin{matrix} a,b,c\in\mathbb{Z}_{11} \\ a=0 \text{ oppure } c=0 \\ \text{e } a,c \text{ non entrambi } 0\end{matrix}\right\} = \left\{\begin{pmatrix} a & 0 \\ 0 & c\end{pmatrix}+I \;\middle|\; \begin{matrix} a,c\in\mathbb{Z}_{11} \\ a=0 \text{ oppure } c=0\end{matrix}\right\} \setminus \{I\}$

Esercizio 2.: Sia $I = \{a_0+a_1x+\dots+a_nx^n \in \mathbb{Z}[x] \mid a_0 \in 18\mathbb{Z}\}$.

(1) I è un ideale di $\mathbb{Z}[x]$:

Si consideri l'applicazione $\phi: \mathbb{Z}[x] \to \mathbb{Z}_{18}$ definita, per $f = a_0+a_1x+\dots+a_nx^n \in \mathbb{Z}[x]$, da $\phi(f) = a_0 + 18\mathbb{Z} = f(0)+18\mathbb{Z}$.

Abbiamo

$\phi = \beta\circ\alpha$ dove $\alpha: \mathbb{Z}[x] \to \mathbb{Z}$ è la valutazione in 0
$f(x) \mapsto f(0)$

e $\beta: \mathbb{Z} \to \mathbb{Z}_{18}$, $a \mapsto a+18\mathbb{Z}$ è l'omomorfismo naturale da $\mathbb{Z}$ a $\mathbb{Z}_{18} = \frac{\mathbb{Z}}{18\mathbb{Z}}$.

Poiché α e β sono omomorfismi suriettivi, segue che ϕ è un omomorfismo suriettivo.

Inoltre, $\mathrm{Ker}(\phi) = I$. Quindi I è un ideale di $\mathbb{Z}[x]$.

(2) Per il teorema di omomorfismo, $\frac{\mathbb{Z}[x]}{I} \cong \mathbb{Z}_{18}$.

Poiché $\mathbb{Z}_{18}$ non è un dominio di integrità, segue che I non è un ideale primo.

Proviamo che I non è principale. Supponiamo, procedendo per assurdo, che sia $I = (g)$ per un $g\in\mathbb{Z}[x]$.

Dato che $x\in I$, segue $g \mid x$ in $\mathbb{Z}[x]$. Ma x è irriducibile

in $\mathbb{Z}[x]$, quindi g invertibile o associato ad x.
Ma anche $18 \in I$; poiché x non divide 18 in $\mathbb{Z}[x]$, segue che g è invertibile. Ma allora $(g) = I = \mathbb{Z}[x]$, contraddizione (infatti $1 \notin I$). Pertanto, I non è principale.

---

(3) $\phi : \mathbb{Z}[x] \to \mathbb{Z}_{18}$, $f \mapsto f(0) + 18\mathbb{Z}$ è un omomorfismo suriettivo.

Per il teorema di corrispondenza, gli ideali massimali di $\mathbb{Z}[x]$ che contengono I sono le retroimmagini tramite ϕ degli ideali massimali di $\mathbb{Z}_{18}$. Dunque gli ideali massimali di $\mathbb{Z}[x]$ che contengono I sono:

$$J_1 = \phi^{-1}\big((2+18\mathbb{Z})\big) = \{ f = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x] \mid a_0 \in 2\mathbb{Z} \}$$

e

$$J_2 = \phi^{-1}\big((3+18\mathbb{Z})\big) = \{ f = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x] \mid a_0 \in 3\mathbb{Z} \}.$$

---

(4) Poiché $\dfrac{\mathbb{Z}[x]}{I} \simeq \mathbb{Z}_{18}$, si ha $\operatorname{char}\left(\dfrac{\mathbb{Z}[x]}{I}\right) = \operatorname{char}(\mathbb{Z}_{18}) = 18$.

Esercizio 3. Si considerino, in $\mathbb{Z}[\sqrt{-14}]$, ~~la~~ fattorizzazioni

$$15 = 3 \cdot 5 = (1+\sqrt{-14})(1-\sqrt{-14}).$$

Proviamo che $3, 5, 1+\sqrt{-14}, 1-\sqrt{-14}$ sono irriducibili in $\mathbb{Z}[\sqrt{-14}]$.

- Non sono invertibili (dato che la norma $N : \mathbb{Z}[\sqrt{-14}] \to \mathbb{N}$, $a+b\sqrt{-14} \mapsto a^2+14b^2$ è moltiplicativa, gli invertibili hanno norma 1; viceversa, gli elementi di norma 1 sono invertibili)
- Se $3 = \alpha\beta$ con $\alpha, \beta \in \mathbb{Z}[\sqrt{-14}]$, α, β non invertibili, allora

$$9 = N(3) = N(\alpha)N(\beta) \quad \text{con} \quad 1 \neq N(\alpha), N(\beta) \in \mathbb{N}.$$

Quindi $3 = N(\alpha) = N(\beta)$; ma $3 \neq a^2 + 14b^2$, $\forall a, b \in \mathbb{Z}$.
Pertanto 3 è irriducibile in $\mathbb{Z}[\sqrt{-14}]$.
Analogamente, sfruttando il fatto che $5 \neq a^2 + 14b^2$, $\forall a, b \in \mathbb{Z}$, si prova che anche 5, $1+\sqrt{-14}$, $1-\sqrt{-14}$ sono irriducibili in $\mathbb{Z}[\sqrt{-14}]$.

Osserviamo che 3 (e 5) non sono associati né a $1+\sqrt{-14}$ né a $1-\sqrt{-14}$ (hanno infatti norme diverse: $N(3) \neq N(1\pm\sqrt{-14})$; $N(5)$ mentre elementi associati hanno la stessa norma).

Dunque $15 = 3\cdot 5 = (1+\sqrt{-14})(1-\sqrt{-14})$ sono due fattorizzazioni in irriducibili "sostanzialmente distinte" e quindi $\mathbb{Z}[\sqrt{-14}]$ non è un dominio a fattorizzazione unica.

- 3 è irriducibile, ma non primo: infatti $3 \mid (1+\sqrt{-14})(1-\sqrt{-14})$ ma 3 non divide $1+\sqrt{-14}$ né $1-\sqrt{-14}$ in $\mathbb{Z}[\sqrt{-14}]$ (dato che $3(a+b\sqrt{-14}) = 3a+3b\sqrt{-14}$).

- Siano $\alpha = 15$, $\beta = 3(1+\sqrt{-14}) = 3+3\sqrt{-14}$; proviamo che α e β non ammettono MCD in $\mathbb{Z}[\sqrt{-14}]$.

Se, per assurdo, d fosse MCD di α e β, allora $N(d) \mid (N(\alpha), N(\beta))$ (poiché $d\mid\alpha$, $d\mid\beta$ in $\mathbb{Z}[\sqrt{-14}]$ implica $N(d)\mid N(\alpha)$ e $N(d)\mid N(\beta)$ in $\mathbb{Z}$) quindi $N(d) \mid 45$.

Inoltre, dato che $3\mid\alpha$, $3\mid\beta$, si ha $3\mid d$ quindi $9 = N(3) \mid N(d)$.
Ma anche $1+\sqrt{-14}\mid\alpha$, $1+\sqrt{-14}\mid\beta$, quindi $1+\sqrt{-14}\mid d$ da cui si deduce $15 = N(1+\sqrt{-14}) \mid N(d)$. Pertanto $[9, 15] = 45 \mid N(d)$.
Si conclude che $N(d) = 45$. Ma $45 \neq a^2+14b^2$, $\forall a,b\in\mathbb{Z}$, contraddizione.

Esercizio 4. $f = (x-1)^2(x^2+1)$, $g = (x-1)^2(x+1)$.
Quindi $(x-1)^2 = x^2-2x+1$ è MCD di f e g.
Pertanto $I = (f,g) = (x^2-2x+1)$.
Sia $\alpha = (x-1)+I$. Allora $\alpha \neq 0_{A/I}$ (dato che $x-1 \notin I$) e $\alpha^2 = (x-1)^2+I = I = 0_{A/I}$.
Dunque α è un elemento nilpotente, non nullo, di A/I.