ALGEBRA 1 — Secondo esonero
15 Giugno 2011
soluzioni

(1) Verificare che l'anello quoziente $\mathbb{Z}_5[x]/(x^3-2)$ possiede divisori dello zero, e determinare tutti i suoi ideali non banali.

Soluzione: Il polinomio $x^3 - 2$ si annulla in $x = 3$ e non è quindi irriducibile in $\mathbb{Z}_5[x]$; pertanto il quoziente $\mathbb{Z}_5[x]/(x^3 - 2)$ non è un dominio d'integrità. Più precisamente, si ottiene $x^3 - 2 = (x + 2)(x^2 + 3x + 4)$ e quindi $[x + 2][x^2 + 3x + 4] = [x^3 - 2] = [0]$.

Per quanto riguarda gli ideali di $\mathbb{Z}_5[x]/(x^3 - 2)$, essi sono in corrispondenza biunivoca con gli ideali di $\mathbb{Z}_5[x]$ che contengono $(x^3 - 2)$. Ora, $\mathbb{Z}_5$ è un campo, e quindi $\mathbb{Z}_5[x]$ è un dominio a ideali principali. Ma allora $I = (d(x)) \supset (x^3-2)$ se e solo se $d(x)$ divide x^3-2. Poiché il generatore di un ideale è determinato a meno di invertibili, possiamo supporre che $d(x)$ sia monico.

La fattorizzazione di x^3-2 in irriducibili di $\mathbb{Z}_5[x]$ è data da $x^3-2 = (x+2)(x^2+3x+4)$, dal momento che $x^2 + 3x + 4$ non ha radici in $\mathbb{Z}_5$. Per il teorema di fattorizzazione unica, gli unici polinomi (monici) che dividono x^3-2 sono $1, x+2, x^2+3x+4$ e $(x+2)(x^2+3x+4)$. Gli ideali di $\mathbb{Z}_5[x]$ che contengono $(x^3 - 2)$ sono quindi $(1) = \mathbb{Z}_5[x]$, $(x + 2)$, $(x^2 + 3x + 4)$ e $(x^3 - 2)$. Gli ideali di $\mathbb{Z}_5[x]/(x^3 - 2)$ si ottengono proiettandoli al quoziente, e sono rispettivamente: $([1]) = \mathbb{Z}_5[x]/(x^3 - 2)$; $([x + 2])$, $([x^2 + 3x + 4])$, $([0])$.

Alcune osservazioni:

- Per verificare che un anello (commutativo) non contiene divisori di zero non bisogna controllare che non sia un campo, ma che non sia un dominio d'integrità. Pertanto l'esercizio richiedeva di mostrare che l'ideale (x^3-2) non è primo, non che non fosse massimale. Ad ogni modo, in un dominio a ideali principali, un ideale non nullo è primo se e solo se è massimale, e quindi la verifica era la stessa.
- Non è vero che i divisori di zero in $\mathbb{Z}_5[x]/(x^3 - 2)$ sono soltanto $[x+2]$ e $[x^2+3x+4]$. In realtà, $[a(x)]$ è un divisore di zero non appena $\mathrm{MCD}(a(x), x^3 - 2) \neq 0$. Questo vuol dire che $a(x)$ ha almeno un primo in comune con $x^3 - 2$. Ricordando che ogni classe di resto contiene uno e un solo elemento di grado minore di 3, i divisori di zero sono tutti e soli gli elementi $[(ax + b)(x + 2)]$ e $[c(x^2 + 3x + 4)]$, con $a, b, c \in \mathbb{Z}_5$.

(2) Sia I l'ideale di $\mathbb{Z}[i]$ generato dagli elementi $14-3i$ e $4+7i$. Trovare, se esistono, tutti gli elementi $\alpha \in \mathbb{Z}[i]$ tali che $I = (\alpha)$.

Soluzione: $\mathbb{Z}[i]$ è un dominio a ideali principali, pertanto I è principale, ed è generato da ciascun massimo comun divisore di $14-3i$ e $4+7i$: in effetti, il massimo comun divisore di due elementi non è unico, ma è determinato a meno di moltiplicazione per invertibili.

Il $\mathrm{MCD}(14-3i, 4+7i)$ si può calcolare in due maniere diverse: si può eseguire l'algoritmo euclideo:

$$\begin{aligned} 14-3i &= (1-2i)(4+7i) - (4+2i) \\ 4+7i &= (1+i)(4+2i) + (2+i) \\ 4+2i &= 2(2+i) + 0 \end{aligned}$$

ottenendo $\mathrm{MCD}(14-3i, 4+7i) = 2+i$. Alternativamente, si può osservare che

$$(14-3i)(14+3i) = 196+9 = 205 = 5 \cdot 41 = (2+i)(2-i)(5+4i)(5-4i),$$

dove tutti e quattro i fattori sono irriducibili. Provando a dividere $14-3i$ per $2 \pm i$ si trova che $14-3i = (2+i)(5-4i)$. Allo stesso modo, da

$$(4+7i)(4-7i) = 16+49 = 65 = 5 \cdot 13 = (2+i)(2-i)(3+2i)(3-2i),$$

si ricava $4+7i = (2+i)(3+2i)$. Il massimo comun divisore si calcola allora moltiplicando i primi comuni ad entrambe le fattorizzazioni, elevati al minimo esponente con il quale compaiono: si ottiene nuovamente $2+i$.

Come già detto sopra, i possibili generatori α dell'ideale I sono tutti e soli gli elementi associati a $2+i$. Si ha quindi $I = (2+i) = (-2-i) = (1-2i) = (-1+2i)$.

(3) Sia $\mathbb{Z}^2 = \mathbb{Z} \oplus \mathbb{Z}$ l'usuale struttura di anello sul prodotto cartesiano $\mathbb{Z} \times \mathbb{Z}$ nella quale le operazioni sono definite componente per componente. Consideriamo i sottoinsiemi

$$I = \{(2a, b) \,|\, a, b \in \mathbb{Z}\}, \qquad J = \{(2a, 3b) \,|\, a, b \in \mathbb{Z}\}.$$

Mostrare che I, J sono ideali di $\mathbb{Z}^2$, e decidere quali delle seguenti affermazioni siano corrette:

- I è massimale;
- I non è primo;
- J è primo ma non massimale;
- J non è primo.

Soluzione: Un'altra notazione per I e J è $I = (2) \oplus (1)$, $J = (2) \oplus (3)$. In generale, $(h) \oplus (k)$ è un ideale di $\mathbb{Z}^2$ per ogni scelta di $h, k \in \mathbb{Z}$: verifichiamolo. Innanzitutto $(0, 0) = (h \cdot 0, k \cdot 0) \in (h) \oplus (k)$. Il sottoinsieme $(h) \oplus (k)$ è inoltre chiuso rispetto alla somma, in quanto $(ha, kb) + (hc, kd) = (h(a + c), k(b + d))$, ed assorbe ovviamente il prodotto per elementi di $\mathbb{Z}^2$, in quanto $(x, y) \cdot (ha, kb) = (h(ax), k(by))$.

Poiché $(2, 1) \cdot (1, 3) = (2, 3) \in (2) \oplus (3)$, si vede subito che J non è un ideale primo, e quindi non può essere nemmeno massimale. I è invece primo, in quanto dire che $(a, b) \cdot (c, d) = (ac, bd) \in I = (2) \oplus (1)$ è equivalente a richiedere la parità di ac; ma allora uno tra a e c deve essere pari.

I è anche massimale. Sia in effetti M un ideale di $\mathbb{Z}^2$ che contiene propriamente I. Allora M contiene almeno un elemento (a, b) con $a = 2h + 1$ dispari. Poiché $(2h, b - 1) \in I \subset M$, M contiene anche $(2h + 1, b) - (2h, b - 1) = (1, 1)$ che è l'unità di $\mathbb{Z}^2$. Pertanto M è tutto $\mathbb{Z}^2$, il che mostra la massimalità di I.

L'esercizio era forse più semplice da risolvere osservando che $(h) \oplus (k)$ è il nucleo dell'omomorfismo $f : \mathbb{Z}^2 \to \mathbb{Z}/(h) \oplus \mathbb{Z}/(k)$ definito da $f(a, b) = ([a]_h, [b]_k)$ — la verifica che si tratta di un omomorfismo di anelli è pressoché immediata, ed il nucleo di un omomorfismo è sempre un ideale.

Poiché f è suriettivo, $\mathbb{Z}/(h) \oplus \mathbb{Z}/(k)$ è isomorfo a $\mathbb{Z}^2/(h) \oplus (k)$. Pertanto $\mathbb{Z}^2/J$ è isomorfo a $\mathbb{Z}/(2) \oplus \mathbb{Z}/(3)$ che non è un dominio d'integrità, e quindi J non è primo; invece $\mathbb{Z}^2/I$ è isomorfo a $\mathbb{Z}/(2) \oplus \mathbb{Z}/(1) \simeq \mathbb{Z}/(2)$ che è un campo, e I è massimale, e di conseguenza anche primo.

In conclusione: è vero che I è massimale; è falso che I non è primo; è falso che J è primo ma non massimale; è vero che J non è primo.

(4) Sia $N \subset \mathbb{Z}^3$ lo $\mathbb{Z}$-sottomodulo generato dagli elementi $(2,2,2)$, $(1,2,4)$, $(3,2,0)$.
- Quanti elementi possiede lo $\mathbb{Z}$-modulo quoziente $M = \mathbb{Z}^3/N$?
- Trovare interi d_1, d_2 con $d_1 \mid d_2$ tali che $M \simeq \mathbb{Z}/(d_1) \oplus \mathbb{Z}/(d_2)$.

Soluzione: è sufficiente applicare l'algoritmo di raddrizzamento studiato a lezione. Si ottiene:

$$\begin{pmatrix} 2 & 1 & 3 \\ 2 & 2 & 2 \\ 2 & 4 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 2 \\ 4 & 2 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 3 \\ 0 & -2 & -4 \\ 0 & -6 & -12 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & -4 \\ 0 & -6 & -12 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & -4 \\ 0 & 0 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

dove abbiamo dapprima scambiato la prima e la seconda colonna; sottratto alla seconda riga 2 volta la prima, e alla terza riga 4 volte la prima; sottratto alla seconda colonna 2 volte la prima e alla terza colonna 3 volte la prima; tolto alla terza riga 3 volte la seconda; infine, sottratto alla terza colonna 2 volte la seconda.

M è quindi isomorfo a $\mathbb{Z}/(1) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(0) \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}$, ed è pertanto infinito. Gli elementi d_1, d_2 cercati sono $d_1 = \pm 2, d_2 = 0$.

(5) Dire per quali $a \in \mathbb{Z}$ il polinomio $3x^3+20ax^2+50a^2x+60$ sia irriducibile, rispettivamente, in $\mathbb{C}[x], \mathbb{R}[x], \mathbb{Q}[x], \mathbb{Z}[x]$. *[Sugg.: il criterio di Eisenstein può tornare utile]*

Soluzione: Nessun polinomio di grado 3 è irriducibile in $\mathbb{C}[x]$ o in $\mathbb{R}[x]$, quindi dobbiamo interessarci soltanto agli ultimi due casi. Osserviamo subito che se a non è un multiplo di 3, il polinomio è primitivo, ed è quindi irriducibile in $\mathbb{Z}[x]$ se e solo se lo è in $\mathbb{Q}[x]$; ma l'irriducibilità in $\mathbb{Z}[x]$ segue facilmente applicando il criterio di Eisenstein con $p = 5$.

Il caso in cui $a = 3k$ è multiplo di 3 è solo apparentemente più complicato: il polinomio non è più primitivo, e quindi non può essere irriducibile in $\mathbb{Z}[x]$. Per quanto riguarda l'irriducibilità in $\mathbb{Q}[x]$, ricordiamo innanzitutto che 3 è invertibile in $\mathbb{Q}[x]$, e quindi è sufficiente valutare l'irriducibilità di

$$3^{-1}(3x^3 + 20ax^2 + 50a^2x + 60) = x^3 + 20kx^2 + 150k^2x + 20,$$

che ha ancora coefficienti interi. Questo polinomio è ora primitivo, e si può ancora applicare il criterio di Eisenstein con $p = 5$.

In conclusione, il polinomio non è mai irriducibile in $\mathbb{C}[x]$, $\mathbb{R}[x]$; sempre irriducibile in $\mathbb{Q}[x]$; è irriducibile in $\mathbb{Z}[x]$ se e solo se 3 non divide a.