A.A. 2015-2016. CORSO DI ALGEBRA 1.
PROFF. P. PIAZZA, E. SPINELLI.
SOLUZIONE ESERCIZI FOGLIO 11.

Esercizio 11.1. Sia $\mathbb{K}$ un campo, $I = (P) \subseteq \mathbb{K}[X]$ un ideale.

(A) Dimostrare che $Q + (P)$ è uno zero-divisore in $\mathbb{K}[X]/(P)$ se e soltanto se $\mathrm{MCD}(Q, P) \neq 1$.
(B) Dimostrare che $Q + (P)$ è nilpotente se e soltanto se $Q \notin (P)$ ed ogni fattore irriducibile della fattorizzazione di P compare nella fattorizzazione di Q con grado non nullo.

Soluzione. Dimostriamo (A). Supponiamo che $Q+(P)$ sia uno zero-divisore non banale. Ne segue che esiste $Q' \notin (P)$ tale che $[Q+(P)]\cdot[Q'+(P)] = (P)$ ovvero $P|Q\,Q'$. Se per assurdo fosse $1 = \mathrm{MCD}(P, Q)$ allora dovrebbe risultare per il Lemma di Euclide $P \mid Q'$ che implicherebbe $Q' \in (P)$. Contraddizione. Supponiamo adesso che $\mathrm{MCD}(P, Q) = D \neq 1$. Scriviamo $P = D\,P'$ e $Q = D\,Q'$. Osserviamo che $P' \notin (P)$ poiché il grado di P' è strettamente inferiore al grado di P e $P' \neq 0$. Abbiamo allora $[Q + (P)] \cdot [P' + (P)] = Q\,P' + (P) = Q'D\,P' + (P) = Q'P + (P) = (P)$.

Dimostriamo (B). Sia $Q + (P)$ un elemento nilpotente di $\mathbb{K}[X]/(P)$. Allora esiste $n \in \mathbb{N}$ tale che $(Q + (P))^n = (P)$ ovvero esiste n tale che $Q^n \in (P)$ ovvero esiste n tale che $P|Q^n$. Sia ora $P = P_1^{h_1} \cdots P_m^{h_m}$ la fattorizzazione di P come prodotto di irriducibili. Allora $P_i|Q^n$, e poiché P_i è irriducibile applicando ripetutamente il lemma di Euclide ne deduciamo che $P_i|Q$. Ne segue che ciascun P_i compare nella fattorizzazione di Q. Viceversa supponiamo che $P = P_1^{h_1} \cdots P_m^{h_m}$ e che ciascun P_i compaia con grado $k_i \geq 1$ nella fattorizzazione di Q. Allora se $m = \mathrm{mcm}(h_1, ..., h_m)$ ne deduciamo che $(Q + (P))^m = (P)$ e dunque $Q + (P)$ è nilpotente in $\mathbb{K}[X]/(P)$. □

Esercizio 11.2. Consideriamo $\mathbb{R}[X]$. Sia $I = (P, Q)$ dove

$$P(X) = X^5 + 3\,X^4 - 41\,X^3 - 63\,X^2 + 256\,X + 420\,; \quad Q(X) = X^4 + 4\,X^3 - 5\,X^2 - 36\,X - 36\,.$$

(A) Trovare un polinomio D che genera l'ideale I.
(B) Descrivere gli elementi nilpotenti e gli zero-divisori di $\mathbb{R}[X]/(D)$.

Soluzione. Cominciamo dal punto (A). Poiché $\mathbb{R}[X]$ è un PID e poiché sappiamo che $(P, Q) = (\mathrm{MCD}(P, Q))$ ci è sufficiente calcolarci l'MCD dei due polinomi. Una verifica diretta (ad esempio sfruttando l'algoritmo di divisione euclidea) consente di determinare l'MCD:

$$\mathrm{MCD}(P, Q) = (X + 2)^2\,(X - 3)$$

Dunque $(P, Q) = ((X + 2)^2(X - 3))$.

Per quanto riguarda (B) possiamo applicare l'esercizio precedente: gli zero divisori sono quindi i polinomi del tipo: $P'\,(X + 2)$, $P''\,(X + 2)^2$, $P'''(X - 3)$, $P''''(X + 2)\,(X - 3)$, dove $(X + 2) \cdot (X - 3) \not| P'$, $(X + 3) \not| P''$, $(X + 2) \cdot (X - 3) \not| P'''$, $(X + 2), (X + 3) \not| P''''$. In particolare gli elementi del tipo $P''''(X + 2)(X - 3)$ con $(X + 2), (X - 3) \not| P''''$ sono gli elementi nilpotenti di $\mathbb{R}[X]/(P)$. □

Esercizio 11.3. Si consideri $\mathbb{Z}_{15}[X]$. Trovare un polinomio di grado 2 con 4 radici distinte in $\mathbb{Z}_{15}$.

Soluzione. Il polinomio $X^2 + \overline{7}\,X = X\,(X + \overline{7}) = (X + \overline{12})\,(X + \overline{10})$ è un polinomio di grado 2 in $\mathbb{Z}_{15}[X]$ con 4 zeri distinti (che danno luogo a 2 fattorizzazioni distinte del polinomio $X^2 + \overline{7}\,X$). □

Esercizio 11. 4. Sia $\mathbb{K}$ un campo. Dimostrare che in $\mathbb{K}[X]$ risulta $P(X) \equiv P(a) \bmod((X-a))$. E' ancora vero in $\mathbb{Z}_n[X]$?

Soluzione. Osserviamo che $Q(X) = P(X) - P(a)$ è un polinomio che si annulla in a: $Q(a) = P(a) - P(a) = 0$. Questo, per il Teorema di Ruffini, è possibile se e soltanto se $(X-a) \mid (P(X) - P(a))$ ovvero se e soltanto se $P(X) \equiv P(a) \bmod((X-a))$. Poiché per l'Esercizio 10.3 sappiamo che il Teorema di Ruffini vale anche nel caso degli anelli di polinomi $\mathbb{Z}_n[X]$ l'argomento precedente funziona anche in questo contesto. □

Esercizio 11. 5. Siano $\mathbb{Z}[i]$ gli interi di Gauss. Determinare un elemento $a + i\,b \in \mathbb{Z}[i]$ tale che $(a + i\,b) = (5\,, -1 + 3\,i)$. Stesso esercizio per $(6\,i, 1 + 5\,i)$ [*Suggerimento. Si sfrutti la nozione di valutazione sull'anello degli interi di Gauss e la divisione col resto*]

Soluzione. Ricordiamo che $val(a + i\,b) = a^2 + b^2$. Consideriamo $val(5) = 5^2 = 25$; osserviamo che 5 non è irriducibile ma ammette invece una fattorizzazione del tipo: $5 = (2 + i)\,(2 - i)$; la valutazione degli interi di Gauss $val(2 \pm i) = 5$ è prima, pertanto non possiamo scomporre tali elementi ulteriormente, essi sono dunque irriducibili. Consideriamo quindi $-1 + 3\,i$; $val(-1 + 3i) = 1 + 9 = 10$. Se tale numero non fosse irriducibile dovremmo aspettarci una fattorizzazione $(a + i\,b)\,(c + i\,d)$ dove $val(a + i\,b) = 2$ e $val(c + i\,d) = 5$. Osserviamo che l'equazione $c^2 + d^2 = 5$ ha le soluzioni intere $\{(\pm 2, \pm 1), (\pm 1, \pm 2)\}$, $\{(\mp 2, \pm 1), (\mp 1, \pm 2)\}$. Sia quindi $c + d\,i = 2 + i$ (qualsiasi altra scelta sarebbe equivalente poiché gli interi di Gauss di valutazione 5 possono tutti essere ottenuti uno dall'altro per moltiplicazione tramite un invertibile di $\mathbb{Z}[i]$). Osserviamo ora che anche gli interi di Gauss di valutazione 2 sono tutti ottenuti uno dall'altro attraverso la moltiplicazione per un invertibile, sono infatti gli elementi $\pm(1 + i)$, $\pm(1 - i) = \pm i\,(1 + i)$. Abbiamo quindi $(-1 + 3\,i) = (2 + i)\,(1 + i)$, ne deduciamo che $\mathrm{MCD}((-1 + 3i), 5) = 2 + i$ e dunque, essendo $\mathbb{Z}[i]$ un anello euclideo e dunque un PID ne deduciamo che $(-1 + 3i, 5) = (2 + i)$.

Per quanto riguarda l'altra coppia di valori, osserviamo preliminarmente che

$$6i = 2 \cdot 3\,i = (1 + i)(1 - i)\,3\,i\,.$$

Ora consideriamo $3\,i$ e calcoliamo la sua valutazione: $val(3\,i) = 9$; se $3\,i$ non fosse irriducibile esso ammetterebbe una fattorizzazione del tipo $3\,i = (a + i\,b) \cdot (c + i\,d)$ dove $val(a + i,\, b) = val(c + i\,d) = 3$. Si osservi ora che l'equazione $x^2 + y^2 = 3$ non ha soluzioni intere., dunque la precedente è una fattorizzazione di $6\,i$ in irriducibili. Consideriamo quindi $1 + 5\,i$. La sua valutazione è 26, se non fosse irriducibile essa dovrebbe essere prodotto di due interi di Gauss $(a + i\,b)$ e $(c + i\,d)$ uno di norma 2 e l'altro di norma 13. Cerchiamo quindi di scrivere $(1 + 5\,i)$ come prodotto di $(a + i\,b)$ per $(1 + i)$ (sappiamo infatti che gli interi di Gauss la cui valutazione 2 sono tutti ottenuti uno dall'altro tramite prodotto per un invertibile): $1 + 5i = (a + i\,b)(1 + i) = (a - b) + i(a + b)$; una soluzione intera del seguente sistema di equazioni è $a = 3$, $b = 2$, pertanto risulta $(1 + 5\,i) = (2 + 3\,i)\,(1 + i)$. L'intero di Gauss $(2 + 3\,i)$ non può essere ridotto ulteriormente poiché la sua valutazione da luogo ad un numero primo e quindi ne deduciamo che $\mathrm{MCD}(6\,i, 1 + 5\,i) = (1 + i)$ da cui $(6\,i, 1 + 5\,i) = (1 + i)$. □

Definizione. Diremo che un anello A è *booleano* se $a^2 = a$ per ogni $a \in A$.

Esercizio 11. 6. [1] Sia A un anello booleano.

(A) Mostrare che $(a + a) = 0_A$, per ogni $a \in A$.
(B) Dimostrare che ogni ideale finitamente generato è un ideale principale. [*Suggerimento. Ragionare per induzione.*]

[1] Tratto da un foglio di esercizi della Prof.ssa P. Gianni, Università di Pisa.

Soluzione. Supponiamo che A sia booleano. Allora $a^2 = a$ per ogni $a \in A \Leftarrow (a+a) = (a+a)^2 = a^2 + a^2 + a^2 + a^2 = a + a + a + a$ da cui segue che $(a+a) = 0_A$.

Sia $I \subseteq A$ un ideale finitamente generato, $I = (a_1, ..., a_n)$. Ragioniamo per induzione; per $n = 1$ il risultato è banale, supponiamo sia vero per n, consideriamo ora un ideale $I = (a_1, ..., a_{n+1})$ generato da $n+1$ elementi. Si osservi che possiamo sostituire alla coppia di generatori a_n, a_{n+1} il generatore $(a_n + a_{n+1} - a_n\, a_{n+1})$: $a_n = a_{n+1} \cdot (a_n + a_{n-1} - a_n\, a_{n+1})$, $a_{n+1} = a_n \cdot (a_n + a_{n+1} - a_n\, a_{n+1})$. Abbiamo quindi $I = (a_1, ..., a_{n+1}) = I(a_1, ..., a_{n-1}, (a_n + a_{n+1} - a_n\, a_{n+1}))$ possiamo quindi applicare l'ipotesi induttiva e concludere che l'ideale I è un ideale principale. □

Esercizio 11. 7. Sfruttando il teorema di corrispondenza fra gli ideali di un anello A contenenti un ideale I e gli ideali di A/I mostrare che A/I è un campo se e soltanto se I è massimale.
Provare che $\mathbb{Z}[i][X]$ non è un PID.

Soluzione. Ricordiamo che segue dalla definizione di ideale e dalla definizione di campo il fatto che $\mathbb{K}$ è un campo se e soltanto se ogni ideale di $\mathbb{K}$ è uguale a $0_{\mathbb{K}}$ oppure a $\mathbb{K}$. Osserviamo quindi che, dato A un anello ed I un suo ideale, per il Teorema di Corrispondenza vi è una corrispondenza biunivoca tra gli ideali contenenti I e gli ideali di A/I. Ne segue che se I è massimale gli unici ideali di $\mathbb{K}$ che lo contengono sono I e $\mathbb{K}$, dunque per il Teorema di Corrispondenza gli unici ideali di A/I sono $\{0_{A/I}\}$ e A/I stesso, dunque A/I è un campo. Viceversa, supponiamo che A/I sia un campo. In particolare non esistono ideali non banali in A/I, pertanto, grazie al Teorema di Corrispondenza possiamo concludere che gli unici ideali di A contenenti I sono A ed I e dunque I è massimale in A.

Ricordiamo che in un PID ogni ideale generato da un irriducibile è massimale. Se $\mathbb{Z}[i][X]$ fosse un PID l'ideale generato da (X) sarebbe dunque massimale e dunque $\mathbb{Z}[i][X]/(X) \simeq \mathbb{Z}[i]$ sarebbe un campo. Contraddizione. □

Esercizio 11. 8. [2] Consideriamo l'anello di polinomi $\mathbb{R}[X]$.

(A) Siano $P, Q, R \in \mathbb{R}[X]$ tre polinomi non costanti tali che

$$\mathrm{MCD}(P, Q) = \mathrm{MCD}(P, R) = \mathrm{MCD}(Q, R) = 1\,.$$

Dimostrare che se

$$(\dagger) \quad P^n + Q^n = R^n$$

allora valgono le seguenti:

$$R^{n-1} \mid (P\,Q' - Q\,P')$$
$$P^{n-1} \mid (Q\,R' - R\,Q')$$
$$Q^{n-1} \mid (P\,R' - R\,P')$$

[*Suggerimento. Moltiplicare per opportuni polinomi e poi sottrarre tra di loro la relazione* (†) *e quella che si ottiene derivando tale relazione*]
(B) Sotto le stesse ipotesi del punto precedente dimostrare che la relazione $P^n + Q^n = R^n$ non ha soluzioni in $\mathbb{R}[X]$ per $n > 2$. [*Suggerimento. Sfruttare quanto dimostrato in* (A) *e ragionare sui gradi*]

Soluzione. Cominciamo dal punto (A). Seguendo il suggerimento scriviamo la relazione (†) e la relazione (che denoteremo in seguito (‡)) ottenuta derivando (†):

$$(\dagger) \quad P^n + Q^n = R^n$$
$$(\ddagger) \quad P^{n-1}P' + Q^{n-1}Q' = R^{n-1}R'$$

Moltiplichiamo ora la prima per P' e la seconda per P e sottraiamo la prima equazione alla seconda; troviamo in questo modo:

$$Q^{n-1}(Q'P - QP') = Q^{n-1}Q'P - Q^nP' = R^{n-1}(R'P - R\,P')$$

[2] Tratto da *A Concrete Introduction to Higher Algebra* di L. Childs.

Poiché $\mathrm{MCD}(Q^{n-1}, R^{n-1}) = 1$ (altrimenti risulterebbe $\mathrm{MCD}(Q, R) \neq 1$) ne deduciamo che

$$Q^{n-1} \mid (R'P - P'R)$$

Le altre tre relazioni si dimostrano in modo analogo a quanto fatto per la precedente.

Per quanto riguarda il punto (B), osserviamo che, se P, Q ed R hanno grado strettamente maggiore di 0 allora $\deg(P'R - R'P) < \deg(R) + \deg(P)$, $\deg(Q'P - P'Q) < \deg(P) + \deg(Q)$ e $\deg(Q'R - R'Q) < \deg(Q) + \deg(R)$. D'altra parte risulta che $(n-1)\deg(Q) \leq \deg(P'R - R'P)$, $(n-1) \cdot (P) \leq \deg(QR' - Q'R)$ e $(n-1)\deg(R) \leq \deg(PQ' - P'Q)$. Deve quindi risultare:

$$(n-1) \cdot (\deg(P) + \deg(Q) + \deg(R)) < 2\,(\deg(P) + \deg(Q) + \deg(R))$$

Poiché stavamo supponendo che $\deg(P), \deg(Q), \deg(R)$ fossero strettamente maggiori di 0 ne deduciamo che questo non è possibile se $n \geq 3$. Ne deduciamo che non esistono soluzioni non costanti all'equazione $P^n + Q^n = R^n$ per $n > 2$. $\square$