A.A. 2015-2016. CORSO DI ALGEBRA 1.
PROFF. P. PIAZZA, E. SPINELLI.
SOLUZIONE ESERCIZI FOGLIO 10.

Esercizio 10. 1. Sia $\mathbb{K}$ un campo.

(A) Mostrare che $\mathbb{K}[X]$ è un dominio ad ideali principali. Cosa possiamo dire di $\mathbb{Z}$? E di $\mathbb{Z}[X]$?
(B) Mostrare che $\mathbb{K}[X,Y]$ non è un PID. [*Suggerimento. Esibire un ideale generato da due polinomi e non principale*]

Soluzione. Cominciamo dal punto (A). Consideriamo un ideale $I \subseteq \mathbb{K}[X]$; sia P un polinomio non nullo di I tale che $\deg(P) = \min\{\deg(Q) \mid Q \in I \setminus \{0\}\}$. Consideriamo ora un polinomio $F \in I \setminus \{0\}$; ricordiamo che, essendo $\mathbb{K}$ un campo, in $\mathbb{K}[X]$ vale la divisione con resto (Capitolo 3, §2, Teorema 1 di *Appunti di Algebra 1* di G. Campanella). Ne segue che esistono unici in $\mathbb{K}[X]$ due polinomi Q ed R tali che $F = Q\,P + R$ con $\deg(R) < \deg(P)$. Ne deduciamo che $R = F - Q\,P \in I$ è un polinomio di I di grado strettamente inferiore al grado di P. Per minimalità del grado di P in $I \setminus \{0\}$ ne deduciamo che $R = 0$ e dunque che $P \mid Q$. Questo dimostra che $I \subseteq (P)$. L'altra inclusione è ovvia. Abbiamo così dimostrato che l'ideale I è principale generato da P. Ne segue che $\mathbb{K}[X]$ è un PID.

Per quanto riguarda $\mathbb{Z}$ si osservi che un ideale di $\mathbb{Z}$ è in particolare un sottogruppo additivo e che un sottogruppo additivo di $\mathbb{Z}$ è dato da $(n) = \{k\,n \mid k \in \mathbb{Z}\}$. Tale sottogruppo additivo è un ideale di $\mathbb{Z}$ come segue da una verifica diretta. Ne deduciamo che ogni ideale di $\mathbb{Z}$ è della forma (n) e dunque è principale.

Arriviamo infine a $\mathbb{Z}[X]$. Mostreremo che non si tratta di un PID. A tal scopo è sufficiente esibire un ideale di $\mathbb{Z}[X]$ che non possa essere generato da un singolo elemento di $\mathbb{Z}[X]$.
Sia $I = (2, X)$. Supponiamo per assurdo che esista $P \in \mathbb{Z}[X]$ tale che $(P) = (2, X)$. In particolare deve risultare che $P \mid 2$, pertanto $\deg(P) = 0$ e $P \in \{\pm 1, \pm 2\}$. Se fosse $P = \pm 1$ avremmo $(P) = \mathbb{Z}[X]$, che è assurdo perché $\pm 1 \notin (2, X)$. Supponiamo quindi $P = 2$ (il caso -2 è identico). Allora avremmo $X \notin (2)$, poiché l'ideale generato da $P = 2$ è l'ideale dei polinomi a coefficienti pari, e questo è assurdo poiché avevamo supposto $(P) = (2, X)$. Ne concludiamo che $(2, X) \neq (P)$ qualsiasi sia $P \in \mathbb{Z}[X]$.

Passiamo al punto (B). Scegliamo i più semplici polinomi di grado ≥ 1 in $\mathbb{K}[X,Y]$, $P(X,Y) = X$ e $Q(X,Y) = Y$. Supponiamo per assurdo che (P,Q) sia generato da un polinomio $F \in \mathbb{K}[X,Y]$. Poiché (X,Y) non contiene le costanti non nulle ne segue che $\deg(F) \geq 1$. Poiché deve risultare $X = S\,F$ e poiché $\deg(F) \geq 1$ ne deduciamo che $S \in \mathbb{K}$, $\deg(F) = 1$ e conseguentemente $F(X,Y) = a\,X + b$ con $a, b \in \mathbb{K}$. Ora poiché $Y \in (F)$ ne deve risultare $Y = T\,F$ e come prima ne deduciamo che $T \in \mathbb{K}^{\cdot}$ e dunque $F(X,Y) = a\,X + b = T\,Y$ questo è assurdo. Ne segue che (X,Y) non è un ideale principale. □

Esercizio 10. 2. [1] Denotiamo con $\mathbb{Z}_n[X]$ l'anello dei polinomi a coefficienti in $\mathbb{Z}_n$. Diremo che $P, Q \in \mathbb{Z}_n[X]$ definiscono la stessa *funzione polinomiale* se $P(\overline{x}) = Q(\overline{x})$ per ogni $\overline{x} \in \mathbb{Z}_n$.

(A) Utilizzando il Piccolo Teorema di Fermat, trovare per ogni numero primo p due polinomi distinti $P, Q \in \mathbb{Z}_p[X]$ che definiscono la stessa funzione polinomiale.
(B) Ragionando come nel punto (A) si esibisca una famiglia numerabile di polinomi distinti che definiscono la stessa funzione polinomiale.
(C) Trovare $Q \in \mathbb{Z}_6[X]$ tale che $Q(X) \neq \overline{3}\,X + \overline{4}\,X^3$ ma $Q(\overline{x}) = \overline{3}\,\overline{x} + \overline{4}\,\overline{x}^3$, per ogni $\overline{x} \in \mathbb{Z}_6$.

[1] Tratto dal libro *A concrete introduction to Higher Algebra* di L. N. Childs.

Soluzione. Partiamo dal punto (A). Ricordiamo che una possibile formulazione del Piccolo Teorema di Fermat è la seguente:

$$\textit{Sia } \overline{x} \in \mathcal{U}(\mathbb{Z}_n) \textit{ allora } (\overline{x})^{\varphi(n)} = \overline{1}.$$

Ricordiamo che se n è un primo allora $\mathcal{U}(\mathbb{Z}_n) = \mathbb{Z}_n \setminus \{\overline{0}\}$, in particolare $\varphi(n) = n - 1$. Ne deduciamo che i polinomi $P(X) = X^n$ e $Q(X) = X$ definiscono la stessa funzione polinomiale su $\mathbb{Z}_n$: sia infatti $\overline{x} \in \mathcal{U}(\mathbb{Z}_n)$, allora $(\overline{x})^n = \overline{x} \cdot (\overline{x})^{\varphi(n)} = \overline{x} \cdot \overline{1} = \overline{x}$, mentre chiaramente $(\overline{0})^{\varphi(n)+1} = \overline{0}$.

Per quanto riguarda (B), osserviamo che possiamo ragionare in modo totalmente analogo a quanto fatto nel punto (A): definiamo $P_k(X) = X^{n^k}$. Allora: $P_k(\overline{0}) = \overline{0}$ mentre

$$P_k(\overline{x}) = P_{k-1}(\overline{x}^n) = P_{k-1}(\overline{x}) = \cdots = P_1(\overline{x}) = P_0(\overline{x}^n) = P_0(\overline{x}) = \overline{x}$$

Pertanto la famiglia $\{P_k\}_{k\in\mathbb{N}}$ è una famiglia di polinomi a due a due distinti che definiscono la medesima funzione polinomiale.

Nel punto (C) si considera invece $\mathbb{Z}_6[X]$, dunque uno $\mathbb{Z}_n[X]$ con $n \in \mathbb{N}$ non primo. Valutando il polinomio $P(X) = \overline{3}\,X + \overline{4}\,X^3$ in ciascun $\overline{x} \in \mathbb{Z}_6$ si può osservare che $P(\overline{x}) = \overline{x}$ per ogni $\overline{x} \in \mathbb{Z}_6$. Scegliamo quindi $Q(X) = X$. □

Esercizio 10.3.
(A) Esibire in $\mathbb{Z}_8[X]$ due polinomi, F e P, di grado 1 tali che $P = Q_1\,F + R_1$ e $P = Q_2\,F + R_2$ con $\deg R_1 = \deg R_2 = 0$ e $Q_1 \neq Q_2$, $R_1 \neq R_2$.
(B) Dimostrare che in $\mathbb{Z}_n[X]$ dati un polinomio P, ed un polinomio F il cui coefficiente direttore sia invertibile, con $\deg P \geq \deg F$, è possibile scrivere $P = Q \cdot F + R$ con $\deg R < \deg P$.
(C) Dimostrare che in $\mathbb{Z}_n[X]$ vale il Teorema di Ruffini.

Soluzione. Lo scopo di tale esercizio è osservare che in $\mathbb{Z}_n[X]$, con n non primo, benché non esista una vera e propria divisione col resto, è possibile ugualmente dimostrare il Teorema di Ruffini. Nel punto (A) si propone un esempio di non unicità di quoziente e resto in una divisione. Nel punto (B) si spiega in che termini si possa parlare di divisione col resto in $\mathbb{Z}_n[X]$. Si arriva quindi al punto (C) dove si chiede di dimostrare il Teorema di Ruffini in $\mathbb{Z}_n[X]$.

Forniamo l'esempio richiesto nel punto (A). In $\mathbb{Z}_8[X]$ si consideri il polinomio $P(X) = \overline{6}\,X + \overline{1}$ e scriviamo: $(\overline{6}\,X + \overline{1}) = \overline{3}\,(\overline{2}\,X + \overline{1}) + \overline{6} = \overline{7}\,(\overline{2}\,X + \overline{1}) + \overline{2}$. Poniamo quindi $F(X) = \overline{2}\,X + \overline{1}$, $Q_1(X) = \overline{3}$, $R_1(X) = \overline{6}$, $Q_2(X) = \overline{7}$, $R_2(X) = \overline{2}$.

Passiamo al punto (B). Sia $P \in \mathbb{Z}_n[X]$ e consideriamo $F \in \mathbb{Z}_n[X]$ un polinomio il cui coefficiente direttore sia un invertibile di $\mathbb{Z}_n$; assumiamo $\deg(P) \geq \deg(F)$. Scriviamo $P(X) = \sum_{i=0}^{m} \overline{a}_i\,X^i$, $F(X) = \sum_{j=0}^{n} \overline{b}_i\,X^i$ con $m \geq n$. Osserviamo che moltiplicando F per $\overline{a}_m\,\overline{b}_n^{-1}\,X^{m-n}$ e sottraendo il risultato a P si ottiene un polinomio di grado strettamente inferiore a $\deg(P)$. Procedendo in questo modo si può replicare la prova valida in $\mathbb{K}[X]$.

Arriviamo quindi al punto (C). Osserviamo che se $(X - \overline{x}) \mid P(X)$ e dunque $P(X) = Q(X)\,(X - \overline{x})$ allora chiaramente $P(\overline{x}) = Q(\overline{x})\,(\overline{x} - \overline{x}) = \overline{0}$. Viceversa, supponiamo che $P(\overline{x}) = \overline{0}$. Per il punto (B) sappiamo che possiamo dividere il polinomio $P(X)$ per il polinomio $(X - \overline{x})$ (il suo coefficiente direttore infatti è chiaramente invertibile in $\mathbb{Z}_n$), pertanto $P(X) = Q(X)\,(X - \overline{x}) + R(X)$ con $\deg(R) \leq 0$ (e dunque $R \in \mathbb{Z}_n$). Abbiamo allora $R = P(\overline{x}) - Q(\overline{x})\,(\overline{x} - \overline{x}) = \overline{0} + \overline{0} = \overline{0}$ dunque $(X - \overline{x}) \mid P(X)$. □

Definizione. Diremo che $\alpha \in \mathbb{C}$ è un *intero algebrico* se esso annulla un polinomio monico in $\mathbb{Z}[X]$ (ad esempio l'unità immaginaria, i, annulla il polinomio monico a coefficienti interi $X^2 + 1$).

Esercizio 10. 4. [2] Sia $\alpha \in \mathbb{C}^*$ un intero algebrico.

(A) Mostrare che esiste un unico polinomio monico in $\mathbb{Z}[X]$ annullato da α e che abbia grado minimo in $\mathcal{I}(\alpha) = \{P(x) \in \mathbb{Q}[X] \mid P(\alpha) = 0\}$. Tale polinomio è detto *polinomio minimo* di α. [*Suggerimento. Sfruttare il fatto che* $\mathbb{Q}[X]$ *è un dominio ad ideali principali ed il Teorema di Gauss*]
(B) Mostrare che l'ideale $\mathcal{I}(\alpha) \cap \mathbb{Z}[X] \subseteq \mathbb{Z}[X]$ costituto dai polinomi a coefficienti interi annullati da α è principale e generato dal polinomio minimo di α.

Soluzione. Per quanto riguarda il punto (A), si osservi innanzitutto che somme e differenze di polinomi che si annullano in α sono ancora polinomi che si annullano in α e che $0 \in \mathcal{I}(\alpha)$. Analogamente il prodotto di un polinomio di $\mathcal{I}(\alpha)$ per un qualunque polinomio in $\mathbb{Q}(X)$ è ancora un polinomio che si annulla in α, pertanto $\mathcal{I}(\alpha)$ è un ideale di $\mathbb{Q}[X]$. Poiché $\mathbb{Q}$ è un campo sappiamo che $\mathbb{Q}[X]$ è un PID e dunque deve esistere un polinomio $P' \in \mathbb{Q}[X]$ tale che $(P') = \mathcal{I}(\alpha)$. Poiché P' divide ogni polinomio che si annulla in α ne segue che $\deg(P')$ è minimale in $\mathcal{I}(\alpha) \setminus \{0\}$. Sia ora $F \in \mathbb{Z}[X] \cap \mathcal{I}(\alpha)$ un polinomio monico. Sappiamo che P' divide F e dunque esiste $Q' \in \mathbb{Q}[X]$ tale che $F(X) = P'(X)\,Q'(X)$. Possiamo allora applicare il Teorema di Gauss ed osservare che vale una simile fattorizzazione , $F(X) = P(X)\,Q(X)$, con P, Q in $\mathbb{Z}[X]$ polinomi rispettivamente associati (in $\mathbb{Q}[X]$) ai polinomi P', Q'. D'altra parte essendo F un polinomio monico, osserviamo che P e Q devono essere anch'essi polinomi monici. Osserviamo inoltre che essendo P e P' polinomi associati risulta $(P) = (P') = \mathcal{I}(\alpha)$ e dunque P ha grado minimale in $\mathcal{I}(\alpha)$ (altrimenti non potrebbe generare). Infine osserviamo che l'unicità segue dal fatto che ogni polinomio di grado minimale in $\mathcal{I}(\alpha)$ è associato a P' e dunque differisce da P' per il coefficiente direttore.

Dimostrare ora l'affermazione del punto (B) è abbastanza facile. Il polinomio P genera l'ideale $\mathcal{I}(\alpha)$ in $\mathbb{Q}[X]$. D'altra parte, essendo il polinomio $P \in \mathbb{Z}[X]$ monico il suo contenuto è uguale ad 1. Questo implica che se $Q \in \mathbb{Q}[X] \setminus \mathbb{Z}[X]$ il polinomio $Q \cdot P \in \mathbb{Q}[X] \setminus \mathbb{Z}[X]$. Ne segue che $\mathbb{Z}[X] \cap \mathcal{I}(\alpha) = \mathbb{Z}[X] \cdot P$, dunque l'ideale $\mathbb{Z}[X] \cap \mathcal{I}(\alpha)$ è principale. □

Esercizio 10. 5. [3] Sia $\alpha \in \mathbb{C}$ un numero intero agebrico e sia $\mathbb{Z}[\alpha]$ il più piccolo sottoanello di $\mathbb{C}$ contenente $\mathbb{Z}$ ed α. Sia P il polinomio minimo di α in $\mathbb{Z}[X]$. Denotiamo con n il suo grado.

(A) Mostrare che ogni elemento di $\mathbb{Z}[\alpha]$ ammette una scrittura della forma $\sum_{i=0}^{n-1} a_i\,\alpha^i$ dove $a_i \in \mathbb{Z}$ e che tale scrittura è unica.
(B) Mostrare che esiste un isomorfismo di anelli $\mathbb{Z}[\alpha] \simeq \mathbb{Z}[X]/(P)$.

Soluzione. Punto (A). Si osservi preliminarmente che $\mathbb{Z}[\alpha]$ è l'insieme delle combinazioni lineari a coefficienti interi delle potenze di α: si tratta infatti di un anello che può essere visto come sottoanello di $\mathbb{C}$ contenente $\mathbb{Z}$ ed α (verificarne la chiusura rispetto a somma e prodotto). Mostriamo che in effetti bastano le potenze $\alpha^0, ..., \alpha^{n-1}$ per generare $\mathbb{Z}[\alpha]$ come gruppo additivo.
Sia infatti P, il polinomio minimo di α, dato da $P(X) = X^n + \sum_{i=0}^{n-1} b_i\,X^i$; poiché α è uno zero di tale polinomio ne segue che $\alpha^n = -\sum_{i=0}^{n-1} b_i\,\alpha^i$. Ne segue che per qualsiasi $m \geq n$ è possibile scrivere α^m come combinazione lineare a coefficienti interi di $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$. Dunque ogni elemento di $\mathbb{Z}[\alpha]$ può essere descritto come combinazione lineare a coefficienti interi di $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$. Andiamo ora a verificare l'unicità di scrittura: supponiamo di avere

$$\sum_{i=0}^{n-1} a_i\,\alpha^i = \sum_{i=0}^{n-1} a'_i\,\alpha^i$$

Se fossero due scritture distinte allora $\sum_{i=0}^{n-1}(a_i - a'_i)\,X^i$ sarebbe un polinomio in $\mathbb{Z}[X]$ di grado strettamente inferiore ad n che si annulla in α, il che è assurdo per via della minimalità di P. Dunque $a_i = a'_i$ per ogni $i = 0, ..., n-1$.

[2] Tratto da un foglio di esercizi a cura di Jacopo Gandini del corso di Algebra 1, A.A. 2010-11.
[3] Tratto da un foglio di esercizi a cura di Jacopo Gandini del corso di Algebra 1, A.A. 2010-11.

Punto (B). Consideriamo la seguente applicazione $\mathscr{V}_\alpha : \mathbb{Z}[X] \to \mathbb{Z}[\alpha]$, $Q \mapsto Q(\alpha)$, ovvero la mappa di valutazione in α. Si tratta di un omomorfismo suriettivo di anelli (verificate questo fatto). Il nucleo di tale omomorfismo è per definizione $\mathcal{I}(\alpha) \cap \mathbb{Z}[X]$ che dall'esercizio precedente sappiamo essere generato in $\mathbb{Z}[X]$ dal polinomio minimo, P. Dal teorema fondamentale di omomorfismo otteniamo quindi il seguente isomorfismo di anelli: $\mathbb{Z}[\alpha] \simeq \mathbb{Z}[X]/(P)$. □

Esercizio 10. 6. Sia A un anello.

(A) Mostrare che se A non ha zero-divisori allora $A[X]$ non ha zero-divisori.
(B) Mostrare che se A ha zero-divisori allora è possibile trovare due polinomi $P, Q \in A[X]$ tali che $\deg(P \cdot Q) < \deg(P) + \deg(Q)$.

Soluzione. Dimostriamo (A). A tal scopo mostreremo che se $A[X]$ ha zero-divisori allora necessariamente A deve avere zero-divisori. Siano $P, Q \in A[X]$ una coppia di polinomi non nulli tali che $P \cdot Q = 0_A$. Si considerino i coefficienti direttori di P e di Q, a_n e b_m (stiamo qui supponendo che P abbia grado n e Q grado m), allora il coefficiente direttore di $P \cdot Q$ è $a_n \cdot b_m$. Tale prodotto è nullo in A, poiché $P \cdot Q = 0_A$, benché né a_n né b_m siano nulli e dunque a_n, b_m sono zero-divisori in A.

Per (B), sulla falsa riga di quanto fatto in (A), si prendano due zero-divisori a, a' e si considerino i polinomi $P(X) = 1_A + a\,X$ e $Q(X) = 1_A + a'\,X$ allora $(1_A + a\,X) \cdot (1_A + a'\,X) = 1_A + (a + a')\,X$ e dunque $\deg(P \cdot Q) = 1 < 2 = \deg(P) + \deg(Q)$. □

Esercizio 10. 7. Sia $\overline{x} \in \mathbb{Z}_n$, consideriamo la seguente mappa (detta *mappa di valutazione in* $\overline{x}$):

$$\mathscr{V}_{\overline{x}} : \mathbb{Z}_n[X] \to \mathbb{Z}_n\ , \quad \mathscr{V}_{\overline{x}}(P) = P(\overline{x})$$

(A) Mostrare che si tratta di un omomorfismo suriettivo di anelli.
(B) Determinare il nucleo di tale omomorfismo. [*Suggerimento. Sfruttare l'esercizio 10.3*]
(C) Sia $n \in \mathbb{N}$ un numero primo. Determinare una famiglia numerabile $\mathcal{F}$ di polinomi con la seguente proprietà: $\forall \overline{i} \in \mathbb{Z}_n$, $\mathscr{V}_{\overline{i}}(P) = \overline{0}$.

Soluzione. Dimostriamo (A). Cominciamo mostrando che si tratta di un omomorfismo:

$$\mathscr{V}_{\overline{x}}(P \cdot Q) = (P \cdot Q)(\overline{x}) = P(\overline{x}) \cdot Q(\overline{x}) = \mathscr{V}_{\overline{x}}(P) \cdot \mathscr{V}_{\overline{x}}(Q), \quad \forall P, Q \in \mathbb{Z}_n[X]\,;$$
$$\mathscr{V}_{\overline{x}}(\overline{1}) = \overline{1}\,; \quad \mathscr{V}_{\overline{x}}(\overline{0}) = \overline{0}\,;$$
$$\mathscr{V}_{\overline{x}}(P + Q) = (P + Q)(\overline{x}) = P(\overline{x}) + Q(\overline{x}) = \mathscr{V}_{\overline{x}}(P) + \mathscr{V}_{\overline{x}}(Q), \quad \forall P, Q \in \mathbb{Z}_n[X]$$

Per la suriettività si osservi che le costanti $\mathbb{Z}_n$ sono contenute in $\mathbb{Z}_n[X]$ e $\mathscr{V}_{\overline{x}}(\overline{y}) = \overline{y}$, per ogni $\overline{y} \in \mathbb{Z}_n$.

Per quanto riguarda (B) sappiamo che $\mathscr{V}_{\overline{x}}(P) = \overline{0}$ se e soltanto se $(X - \overline{x}) \mid P$ (Esercizio 10.3). Ne deduciamo che $\ker(V_{\overline{x}}) = (\,(X - \overline{x})\,)$.

Passiamo al punto (C). Per $n \in \mathbb{N}$ primo si chiede di individuare una famiglia numerabile $\mathcal{F}$ tale che ciascun elemento della famiglia definisca la funzione polinomiale banale. Nuovamente ci viene incontro un esercizio precedente (Esercizio 10.2). Sappiamo infatti che la famiglia $\{P_k\}_{k \in \mathbb{N}}$ data da $P_k(X) = X^{n^k}$ definisce la stessa funzione polinomiale $P_k(\overline{x}) = P_0(\overline{x}) = \overline{x}$ per ogni $k \in \mathbb{N}$. Definiamo allora $Q_k(X) = P_k(X) - P_0(X) = X^{n^k} - X$ e si osservi che tale famiglia verifica $\mathscr{V}_{\overline{i}}(Q_k) = \overline{0}$ per ogni $k \in \mathbb{N}$. □