A.A. 2015-2016. CORSO DI ALGEBRA 1.
PROFF. P. PIAZZA, E. SPINELLI.
ESERCITAZIONI. 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*]

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 $\overline{x} \in \mathbb{Z}_6$.

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.

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 $\mathcal{I}(\alpha) \cap \mathbb{Z}[X] \subseteq \mathbb{Z}[X]$ costituito dai polinomi a coefficienti interi annullati da α è principale e generato dal polinomio minimo di α.

[1] Tratto dal libro *A concrete introduction to Higher Algebra* di L. N. Childs.
[2] Tratto da un foglio di esercizi a cura di Jacopo Gandini del corso di Algebra 1, A.A. 2010-11.

ESERCIZI PER CASA

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 $\mathbb{Z}[\alpha] \simeq \mathbb{Z}[X]/(P(X))$.

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 $\deg(P \cdot Q) < \deg(P) + \deg(Q)$.

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: $\forall \overline{i} \in \mathbb{Z}_n$, $\mathscr{V}_{\overline{i}}(P) = \overline{0}$.

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