TRENTO, A.A. 2022/23
CORSO DI ALGEBRA B
FOGLIO DI ESERCIZI # 7

Esercizio 7.1. Sia F un campo, e

$$a(x) = a_0 + a_1 x + \cdots + x^n \in F[x]$$

un polinomio monico, non costante.

Si mostri che $x + (a(x)) \in F[x]/(a(x))$ è radice del polinomio

$$\overline{a}(y) = \overline{a_0} + \overline{a_1} y + \cdots + y^n \in \overline{F}[y],$$

ove $\overline{F} = \{\, \lambda + (a(y)) : \lambda \in F \,\}$ 'e un campo isomorfo a F.

Esercizio 7.2. Sia F un campo, e

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 \\ & & & & \ddots & & \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 \\ -a_0 & -a_1 & -a_2 & -a_3 & \dots & -a_{n-2} & -a_{n-1} \end{bmatrix}$$

una matrice a coefficienti in F.

(1) Si mostri che A è radice del polinomio

$$a = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n.$$

Qui le costanti $a \in F$ vanno interpretate come matrici scalari.

(2) Si mostri che la matrice A non è radice di alcun polinomio di grado minore di n, e che dunque a è il polinomio minimo di A su F.

Esercizio 7.3. Sia F un campo, e $a \in F[x]$ un polinomio monico, non costante.

Si mostri che esistono una estensione B di F e $\alpha \in B$ tali che a sia il polinomio minimo di α su F; in particolare $a(\alpha) = 0$.

Esercizio 7.4. Sia F un campo, $f \in F[x]$ monico e non costante..

(1) Si definisca il campo di spezzamento di f su F.
(2) Si dimostri che questo campo di spezzamento esiste.

Esercizio 7.5.

(1) Si definisca la caratteristica di un anello con unità.
(2) Si mostri che se un anello ha caratteristica zero, allora contiene un sottoanello isomorfo a $\mathbf{Z}$, mentre se ha caratteristica $m > 0$, allora contiene un sottoanello isomorfo a $\mathbf{Z}/m\mathbf{Z}$.
(3) Si mostri che la caratteristica di un dominio o è 0, o è un numero primo.
(4) Si mostri che se l'anello A ha caratteristica $m > 0$, allora per ogni $a \in A$ si ha $m \cdot a = 0$

Esercizio 7.6. Sia E un campo di caratteristica zero. Dunque contiene un sottoanello isomorfo a $\mathbf{Z}$.

Mostrate che allora E contiene un sottoanello isomorfo a $\mathbf{Q}$.

(SUGGERIMENTO: Sfruttate il fatto che $\mathbf{Q}$ è il campo dei quozienti di $\mathbf{Z}$, e la proprietà universale del campo dei quozienti.)

Esercizio 7.7. Sia F un campo. Per

$$a = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$$

di definisca la *derivata formale*

$$a' = a_1 + 2a_2 x + \cdots + (n-1)a_{n-1}x^{n-2} + n a_n x^{n-1}.$$

(1) Si mostri che per $a, b \in F[x]$ e $\lambda, \mu \in F$ si ha

$$(\lambda a + \mu b)' = \lambda a' + \mu b', \qquad (ab)' = a'b + ab'.$$

(2) Si ricordino le definizioni di radice semplice e multipla.
(3) Sia $f \in F[x]$ un polinomio monico, non costante, e K un campo , estensione di F.
   (a) Si mostri che se $\alpha \in K$ è una radice multipla di f, allora $x - \alpha \mid f'$, e dunque $x - \alpha \mid \gcd(f, f')$.
   (b) Si mostri che se $\alpha \in K$ è una radice semplice di f, allora $x - \alpha n \mid f'$, e dunque $x - \alpha \nmid \gcd(f, f')$.
(4) Sia $f \in F[x]$ un polinomio monico, non costante. Si mostri che se $g = \gcd(f, f')$ è un polinomio non costante, e K è una estensione di F in cui g ha una radice α, allora α è una radice multiple di f.

Esercizio 7.8.

(1) Sia E un campo finito.
   (a) Si mostri che la caratteristica di E è un numero primo p, e dunque E è una estensione di $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.
   (b) Si mostri che la dimensione $|E : \mathbf{F}_p| = n$ è finita.
   (c) Si mostri che $| E | = p^n$.
   (d) Si mostri che E è l'insieme delle radici di $x^{p^n} - x \in \mathbf{F}_p[x]$.
(2) Sia A un anello commutativo con unità di caratteristica il primo p. Si mostri che per $a, b \in A$ vale

$$(a+b)^p = a^p + b^p.$$

(3) Siano p un primo, e $n > 0$ un intero. Sia K un campo di spezzamento di $x^{p^n} - x \in \mathbf{F}_p[x]$, e sia

$$\mathcal{E} = \left\{ \alpha \in K : \alpha^{p^n} = \alpha \right\}.$$

   (a) Si mostri che $\mathcal{E}$ è un sottoanello di K.
   (b) Si mostri che $\mathcal{E}$ è un campo.
   (c) Si mostri che $\mathcal{E}$ ha p^n elementi.

Esercizio 7.9 (Facoltativo). Sull'insieme $X = \mathbf{N} \times \mathbf{N}$ si consideri la relazione R data da

$$(a, b)R(c, d) \iff a + d = b + c.$$

(1) Si mostri che R è una relazione di equivalenza.
(2) Si mostri che ogni classe si scrive in modo unico nella forma

$$\begin{cases} [(e, 0)] & \text{per } a \geq 0 \\ [(0, e)] & \text{per } a < 0 \end{cases}$$

(SUGGERIMENTO: Una classe $[(a, b)]$ è del primo tipo quando $a \geq b$, e allora $e = a - b$, è del secondo tipo quando $a < b$, e allora $e = b - a$.)
(3) Si mostri che le operazioni su X/R

$$[(a, b)] + [(c, d)] = [(a + c, b + d)], \quad [(a, b)] \cdot [(c, d)] = [(ac + bd, ad + bc)]$$

sono ben definite, e inducono su X/R una struttura di anello commutativo, con zero $[(0, 0)]$ e unità $[(1, 0)]$.
(4) Si mostri che la funzione

$$X/R \to \mathbf{Z}$$
$$[(a, b)] \mapsto a - b$$

è ben definita, ed è un isomorfismo di anelli. Dunque questa costruzione può essere usata per costruire l'anello degli interi partendo dai numeri naturali.

Esercizio 7.10 (Facoltativo). Questo esercizio è una variazione insiemistica sull'Esercizio 7.1. Vogliamo trovare una estensione di F, e non di $\overline{F}$ in cui $a(y)$, e non $\overline{a}(y)$ abbia una radice.

Se grado$(a) = n$, consideriamo l'insieme

$$B = \left\{ b_0 + b_1 x + \ldots b_n x^{n-1} : b_i \in F \right\},$$

e la biiezione

$$\varphi : B \to F[x]/(a(x))$$
$$b \mapsto b + (a(x)).$$

Usiamo φ per definire, mediante trasporto di struttura, operazioni su B che lo rendano un anello isomorfo a $F[x]/(a(x))$; in sostanza le operazioni su B sono la somma e il prodotto modulo $a(x)$.

Mostrate che B risulta una estensione di F in cui $a(y)$ ha radice x.