TRENTO, A.A. 2022/23
CORSO DI ALGEBRA B
FOGLIO DI ESERCIZI # 4

Esercizio 4.1. Sia B un anello commutativo con unità 1, estensione del campo F, con $1 \in F$.

Mostrate come si può vedere B come spazio vettoriale su F.

Esercizio 4.2. Si ricordi che un ideale I di un anello A è detto principale se $I = (a) = \{ au : u \in A \}$ per qualche $a \in A$.

(1) Si dia la definizione di dominio a ideali principali.
(2) Si mostri che un dominio euclideo è un dominio a ideali principali, facendo vedere che se $I \neq \{ 0 \}$ è un ideale del dominio euclideo A, allora $I = (a)$, ove a è un elemento di I di norma minima fra gli elementi diversi da 0 di I.
(3) Come caso particolare, sia $I \neq \{ 0 \}$ un ideale dell'anello $F[x]$ dei polinomi, ove F è un campo. Si mostri che $I = (a)$, ove a è un polinomio di grado minimo fra gli elementi diversi da zero di I, che può essere scelto monico.

Esercizio 4.3. Sia A un dominio, $a, b \in A$.

(1) Su mostri che $a \in (a)$
(2) Si mostri che sono equivalenti
    (a) $a \mid b$,
    (b) $(a) \ni b$, e
    (c) $(a) \supseteq (b)$.
(3) Si mostri che sono equivalenti
    (a) $(a) = (b)$,
    (b) $a \mid b$ e $b \mid a$, ovvero $b = \varepsilon a$ per una unità ε.
(4) Si mostri che $(1) = A$.
(5) Si mostri che sono equivalenti
    (a) $(a) = A$, e
    (b) a è una unità.
(6) Sia F un campo, $I \neq \{ 0 \}$ un ideale di $F[x]$. Si mostri che esiste un unico $m \in F[x]$ monico tale che $I = (m)$.

Esercizio 4.4. Sia $\varphi : A \to B$ un morfismo di gruppi (scritti moltiplicativamente).

Si mostri che sono equivalenti

(1) φ è iniettivo, e
(2) $\ker(\varphi) = \{ 1 \}$.

Esercizio 4.5. Sia $\varphi : A \to B$ un morfismo di anelli.

Si mostri che sono equivalenti

(1) φ è iniettivo, e
(2) $\ker(\varphi) = \{ 0 \}$.

Esercizio 4.6. Sia B/F una estensione di un campo F, e $\alpha \in B$. Si dica quando α è algebrico e quando è trascendente su F.

Esercizio 4.7. Sia B/F una estensione di un campo F, e $\alpha \in B$ trascendente su F.

Si mostri che $F[\alpha]$ è isomorfo all'anello dei polinomi $F[x]$.

Esercizio 4.8. Sia B/F una estensione del campo F, e $\alpha \in B$ algebrico su F.

Sia

$$\begin{aligned} v_\alpha : F[x] &\to F[\alpha] \\ f &\mapsto f(\alpha) \end{aligned}$$

il morfismo di valutazione.

(1) Si mostri che $\ker(v_\alpha) \neq \{ 0 \}$.
(2) Si mostri che $\ker(v_\alpha) = (m)$ per un polinomio monico m.
(3) Si mostri che m soddisfa le seguenti proprietà
   (a) m è monico,
   (b) $m(\alpha) = 0$,
   (c) se $f(\alpha) = 0$, e $f \neq 0$, allora $\text{grado}(m) \leq \text{grado}(f)$.
(4) Mostrate come per un polinomio monico $m \in F[x]$ siano anzi equivalenti le seguenti condizioni:
   (a) $\ker(v_\alpha) = (m)$,
   (b) (i) $m(\alpha) = 0$,
      (ii) se $f(\alpha) = 0$, e $f \neq 0$, allora $\text{grado}(m) \leq \text{grado}(f)$.
(5) Si mostri che se m è il polinomio definito in (2), per $f \in F[x]$ sono equivalenti
   (a) $f(\alpha) = 0$,
   (b) $m \mid f$.
(6) Si mostri che un m che soddisfi le condizioni di (3) è unico.

Esercizio 4.9. (Questo l'abbiamo già visto ad Algebra A, ma è utile ricordarlo adesso)

Sia F un campo, $F[x]$ l'anello dei polinomi a coefficienti in F.

(1) Si mostri che gli elementi di $F[x]$ di grado zero sono tutte e sole le costanti non nulle, dunque gli elementi di $F^\star = F \setminus \{ 0 \}$, visti come polinomi in cui non compare la x.
(2) Si mostri che gli elementi invertibili di $F[x]$ sono le costanti non nulle.

Esercizio 4.10. Sia F un campo, $A = F[x]$ l'anello dei polinomi, e $a \in A$, con $a \neq 0$, e a non una unità.

Indichiamo con $a \sim b$ il fatto che a e b siano *associati*, cioè $a \mid b$ e $b \mid a$.

Si mostri che le seguenti proprietà sono equivalenti, e significano che a è *riducibile*, cioè non irriducibile:

(1) esiste $d \mid a$, tale che d non è una costante non nulla, e $d \not\sim a$;
(2) esistono $u, v \in A$ tali che $a = uv$, e né u né v è una costante non nulla;
(3) esistono $u, v \in A$ tali che $a = uv$, e $u, v \not\sim a$;
(4) esistono $u, v \in A$ tali che $a = uv$, e $\text{grado}(u), \text{grado}(v) > 0$;
(5) esistono $u, v \in A$ tali che $a = uv$, e $\text{grado}(u), \text{grado}(v) < \text{grado}(a)$;

Esercizio 4.11. Sia B/F una estensione del campo F, e $\alpha \in B$ algebrico su F, con polinomio minimo m di grado k. Scriviamo $[a] = a + (m)$ per classe laterale di a in $F[x]/(m)$.

(1) Si mostri che per $a, r \in F[x]$, ove $r = 0$, o grado$(r) <$ grado(m), sono equivalenti
   (a) $[a] = [r]$, e
   (b) r è il resto della divisione di a per m.

   (SUGGERIMENTO: Esattamente come per il caso degli interi visto ad Algebra A.)

(2) Si mostri che gli elementi di $F[x]/(m)$ si scrivono in modo unico nella forma $[r] = r + (m)$, ove $r = 0$, o grado$(r) <$ grado(m), dunque nella forma

$$[r_0 + r_1 x + \cdots + r_{k-1} x^{k-1}],$$

   per $r_i \in F$.

   (SUGGERIMENTO: Dal punto precedente, ogni $[a] \in F[x]/(m)$ si scrive nella forma data, e si scrive in modo unico per l'unicità del resto.)

(3) Si mostri che gli elementi di $F[\alpha]$ si scrivono in modo unico nella forma

$$r_0 + r_1 \alpha + \cdots + r_{k-1} \alpha^{k-1}, \tag{1}$$

   per $r_i \in F$. Dunque

$$1, \alpha, \dots, \alpha^{k-1}$$

   sono una base di $F[\alpha]$ come spazio vettoriale su F.

   (SUGGERIMENTO: Primo modo: si prende il punto precedente, e si applica la valutazione v_α. Secondo modo, che ripete in parte quanto già visto: se $a(\alpha) \in F[\alpha]$, per $a \in F[x]$, divido a per m ottenendo $a = mq + r$, con $r = 0$, o grado$(r) <$ grado(m). Valutando in α, ottengo $a(\alpha) = m(\alpha)q(\alpha) + r(\alpha) = r(\alpha)$, dato che $m(\alpha) = 0$. Dunque $a(\alpha)$ si scrive nella forma (1). Ora $1, \alpha, \dots, \alpha^{k-1}$ sono linearmente indipendenti su F perché se

$$r_0 + r_1 \alpha + \cdots + r_{k-1} \alpha^{k-1} = 0,$$

   allora il polinomio $r = r_0 + r_1 x + \cdots + r_{k-1} x^{k-1}$ si annulla su α, e dunque deve essere il polinomio nullo, altrimenti ha grado minore del grado k di m,che è il polinomio minimo.)

(4) Solo per ricordare che la dimensione di una estensione B/F si chiama *grado* dell'estensione stessa, e si indica con $|\,B : F\,|$. Abbiamo quindi visto il seguente fatto, che spiega l'uso del termine *grado* per denotare una *dimensione*:

   Se α è algebrico su F, allora il grado $|\,F[\alpha] : F\,|$ dell'estensione $F[\alpha]/F$ è eguale al grado del polinomio minimo di α su F.

Esercizio 4.12. Sia B/F un'estensione del campo F, e $\alpha \in B$ algebrico su F.

(1) Sia $f \in F[x]$ monico, tale che $f(\alpha) = 0$. Si mostri che se f è irriducibile in $F[x]$, allora f è il polinomio minimo di α su F.

(2) Si dia un esempio di polinomio minimo che non è irriducibile.

(SUGGERIMENTO: Rendo espliciti un paio di passaggi su cui avevo sorvolato nell'esempio che avevo dato in classe. Consideriamo l'anello $M = M_{2\times 2}(\mathbf{Q})$ delle matrici a coefficienti in $\mathbf{Q}$. Si vede subito che l'insieme delle matrici scalari

$$S = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} : a \in \mathbf{Q} \right\}$$

è un sottoanello di M isomorfo a $\mathbf{Q}$, dunque S è un campo. Ora consideriamo la matrice

$$\alpha = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},$$

e il sottoinsieme

$$B = \{ s + t\alpha : s, t \in S \} = \left\{ \begin{bmatrix} a & c \\ 0 & a \end{bmatrix} : a. \in \mathbf{Q} \right\}$$

di M. Sfruttando il fatto che $sm = ms$ per ogni $s \in S$ e $m \in M$, e che $\alpha^2 = 0$, si vede agevolmente che B è un anello commutativo, estensione del campo S. A lezione ho fatto vedere che il polinomio minimo di α su S è x^2.)

Esercizio 4.13. Sia F un campo, $m \in F[x]$ un polinomio monico. Si mostri che

$$F[x]/(m) \begin{cases} \text{è un campo} & \text{se } m \text{ è irriducibile in } F[x], \\ \text{non è un dominio} & \text{se } m \text{ è riducibile.} \end{cases}$$