TRENTO, A.A. 2019/20
CORSO DI ALGEBRA A
FOGLIO DI ESERCIZI # 11

Esercizio 11.1. Si mostri che, nelle notazioni del foglio precedente, l'immagine $v_\alpha(A[x]) = A[\alpha]$ del morfismo di valutazione è il più piccolo sottoanello di B che contenga A e α.

Esercizio 11.2. Sia A un dominio, $a, b \in A$.

Definiamo su A la divisibilità nel solito modo: si dice che b divide a (in simboli $b \mid a$) se esiste $c \in A$ tale che $a = bc$.

(1) Si mostri che la divisibilità è riflessiva e transitiva.
(2) Si mostri che sono equivalenti
   (a) $a \mid b$ e $b \mid a$,
   (b) $a = b\varepsilon$, con $\varepsilon \in A$ invertibile.
(3) Due elementi $a, b \in A$ si dicono *associati* (in simboli, $a \sim b$) se valgono le proprietà equivalenti del punto precedente.

   Mostrate che $\sim$ è un relazione di equivalenza. Questo segue dal prossimo punto, che è legato all'esercizio seguente.
(4) Sia $A \neq \emptyset$ un insieme, e R una relazione su A che sia riflessiva e transitiva. Mostrate che la relazione Q su A definita, per $a, b \in A$, da

$$aQb \text{ se e solo se } aRb \text{ e } bRa,$$

   è una relazione di equivalenza.

Esercizio 11.3 (Del tutto facoltativo, ma utile da sapere).

Sia $A \neq \emptyset$ un insieme, e $R \subseteq A \times A$ una relazione su A. Dunque pensiamo R come un sottoinsieme di $A \times A$, e aRb equivale a $(a, b) \in R$.

(1) Una relazione R è riflessiva se e solo se $\Delta \subseteq R$, ove $\Delta = \{ (a, a) : a \in A \}$ è la *diagonale*.
(2) La più piccola relazione riflessiva che contenga R è $S = R \cup \Delta$.

   In altre parole, per $a, b \in A$ vale

$$aSb \text{ se e solo se } \begin{cases} aRb, & \text{oppure} \\ a = b. \end{cases}$$

(3) Una relazione R è simmetrica se e solo se $R = R^{\text{inv}}$, ove per una relazione T si scrive

$$T^{\text{inv}} = \{ (a, b) : (b, a) \in T \}.$$

(4) La *più piccola relazione simmetrica che contenga* R è $Q = R \cup R^{\text{inv}}$.

   In altre parole, per $a, b \in A$ vale

$$aQb \text{ se e solo se } aRb \text{ oppure } bRa,$$

(5) La *più grande relazione simmetrica contenuta in* R è $Q = R \cap R^{\text{inv}}$.

   In altre parole, per $a, b \in A$ vale

$$aQb \text{ se e solo se } aRb \text{ e } bRa,$$

(6) La più piccola relazione transitiva che contenga R è la relazione S definita come

$$aSb \qquad \text{se e solo se} \qquad \begin{array}{l}\text{esistono } a_1 = a, a_2, \ldots, a_n, a_{n+1} = b \text{ tali che} \\ a_i R a_{i+1} \text{ per } i \leq n.\end{array}$$

(7) La più piccola relazione di equivalenza che contenga R è... lascio a voi la formulazione.

Esercizio 11.4. Sia A un dominio, $A[x]$ l'anello dei polinomi, $a \in A[x]$.

Identifichiamo come d'uso A col sottoanello di $A[x]$ dei polinomio costanti, cioè quelli in cui non compare x.

(1) Si mostri che sono equivalenti
   (a) a è un polinomio di grado 0, e
   (b) a è una costante non nulla.
(2) Si mostri che sono equivalenti
   (a) a è invertibile in $A[x]$, e
   (b) a è una costante non nulla, dunque $a \in A$, e a è invertibile in A.

   Come caso particolare, si mostri che gli elementi invertibili di $\mathbf{Z}[x]$ sono $1, -1$.
(3) Sia ora $A = F$ un campo, e $a \in F[x]$. Si mostri che sono equivalenti
   (a) a è invertibile in $F[x]$,
   (b) a è un polinomio di grado 0, e
   (c) a è una costante non nulla.
(4) Si mostri che se $a, b \in F[x]$, allora $a \mid b$ e $b \mid a$ se e solo se $a = b\varepsilon$, con $\varepsilon \in F$ una costante non nulla.

Esercizio 11.5. Data per buona la parte dell'esistenza, che si fa con l'algoritmo noto, del seguente teorema, si dimostri l'*unicità*.

Teorema. Sia F un campo, e $a, b \in F[x]$, con $b \neq 0$. Allora esistono unici $q, r \in F[x]$ tali che

$$\begin{cases} a = bq + r \\ r = 0 \text{ } \textit{oppure} \text{ } \deg(r) < \deg(b). \end{cases}$$

(Suggerimento: Sia $a = bq_1 + r_1 = bq_2 + r_2$, con gli r_i che soddisfano le condizioni. Dunque

$$b(q_1 - q_2) = r_1 - r_2.$$

Se $q_1 = q_2$, allora anche $r_1 = r_2$. Se invece fosse $q_1 \neq q_2$, allora sarebbe anche $r_1 \neq r_2$, e si avrebbe

$$\deg(b(q_1 - q_2)) = \deg(b) + \deg(q_1 - q_2) \geq \deg(b)$$

mentre $\deg(r_1 - r_2)$ per un esercizio precedente è minore di $\deg(b)$.)

Esercizio 11.6. Si applichi l'algoritmo di Euclide ai polinomi

$$x^2 + 1, x^3 - 2 \in \mathbf{Q}[x]$$

e si usi il risultato per razionalizzare

$$\frac{1}{\sqrt[3]{2}^2 + 1},$$

cioè per scriverlo nella forma

$$c_0 + c_1\sqrt[3]{2} + c_2\sqrt[3]{2}^2$$

per opportuni $c_i \in \mathbf{Q}$.

Esercizio 11.7. Si consideri l'anello $\mathbf{Z}[x]$ dei polinomi a coefficienti interi.

Si mostri che non è possibile fare la divisione con resto del polinomio x per il polinomio 2.

(SUGGERIMENTO: Se fosse possibile, esisterebbero $q, r \in \mathbf{Z}[x]$ tali che $x = 2q+r$, e $r = 0$, oppure grado$(r) <$ grado$(2) = 0$. Quest'ultima condizione è impossibile, dato che il grado di un polinomio è un intero non negativo, dunque deve essere $r = 0$, cioè $x = 2q$ per un certo $q = q_0 + q_1x + \dots$. Ma allora, confrontando i coefficienti, si ha $1 = 2q_1$, con $q_1 = 1/2 \in \mathbf{Z}$, una contraddizione.)

Esercizio 11.8. Sia A un anello commutativo con unità, e $A[x]$ l'anello dei polinomi a coefficienti in A.

Sia $b \in A[x]$ un polinomio di grado n, con b_n invertibile in A.

Si mostri che in $A[x]$ si può fare la divisione con resto di ogni polinomio $a \in A[x]$ per b.

Esercizio 11.9. Sia A un dominio.

(1) Si definisca il concetto di radice di $a \in A[x]$.
(2) Si enunci e si dimostri la Regola di Ruffini: sono equivalenti, per un polinomio $a \in A[x]$ e $\alpha \in A$
   (a) α è una radice di a, ovvero $v_\alpha(a) = 0$, e
   (b) $x - \alpha \mid a$.
(3) Si mostri che se $a \in A[x]$ ha grado n, allora a ha al più n radici distinte in A.
(4) Si dia un esempio di un anello commutativo B con unità, e di un polinomio $b \in B[x]$ che ha grado 2 ma più di 2 radici in B.

Esercizio 11.10. Sia $\alpha \in \mathbf{C}$ con la proprietà che

(1) $\alpha \notin \mathbf{Q}$, e
(2) α è radice di un polinomio $x^2 + c_1x + c_0 \in \mathbf{Z}[x]$.

(Ad esempio $\alpha = \sqrt{2}, \sqrt{3}, i, \sqrt{-5}$.)

Si mostri che $\mathbf{Z}[\alpha] = \{\, a_0 + a_1\alpha : a_0, a_1 \in \mathbf{Z} \,\}$, e che la scrittura degli elementi di $\mathbf{Z}[\alpha]$ nella forma $a_0 + a_1\alpha$ è unica.

Esercizio 11.11. Sia dia la definizione di elemento irriducibile e elemento primo in un dominio.

Esercizio 11.12. Sia A un dominio, $a, b, c \in A$, con $a \neq 0$, e sia $a = bc$.

Si mostri che

- se b è una unità, allora c è associato ad a;
- se b è associato ad a, allora c è una unità.

Esercizio 11.13. Sia A un dominio, e $a \in A$, che non sia né zero, né una unità.

Si mostri che sono equivalenti

(1) a è irriducibile, ovvero i suoi soli divisori sono gli elementi invertibili, e i cosiddetti elementi *associati* ad a.
(2) Per ogni $u, v \in A$, se $a = uv$, allora o u o v è invertibile.
(3) Per ogni $u, v \in A$, se $a = uv$, allora o u o v è associato ad a.
(4) Per ogni $u, v \in A$, se $a = uv$, allora o u è invertibile, o u è associato ad a.
(5) Per ogni $u, v \in A$, se $a = uv$, allora
    - o u è invertibile, e v è associato ad a,
    - o u è associato ad a, e v è invertibile.

Esercizio 11.14. Sia A un dominio. Si mostri che se $a \in A$ è primo, allora è anche irriducibile.

Esercizio 11.15. Sia A un dominio.

(1) Definite il concetto di norma su A.
(2) Mostrate che se N è una norma su A, e $a \in A$ è una unità, allora $N(a) = 1$.
(3) Definite il concetto di norma speciale.
(4) Mostrate che la funzione valore assoluto $N(a) = |\, a \,|$ è una norma speciale su $\mathbf{Z}$.

Esercizio 11.16.

(1) Sia F un campo. Mostrate che la funzione $N : F[x] \to \mathbf{N}$ data da
$$\begin{cases} N(0) = 0 \\ N(a) = 2^{\text{grado}(a)} & \text{se } a \neq 0 \end{cases}$$
è una norma speciale su $F[x]$.
(2) Mostrate che la funzione $N : \mathbf{Z}[x] \to \mathbf{N}$ data da
$$\begin{cases} N(0) = 0 \\ N(a) = 2^{\text{grado}(a)} & \text{se } a \neq 0 \end{cases}$$
è una norma che non è speciale su $\mathbf{Z}[x]$.
(3) Mostrate che la funzione $N : \mathbf{Z}[x] \to \mathbf{N}$ data da
$$\begin{cases} N(0) = 0 \\ N(a) = |\, a_n \,| \cdot 2^n & \text{se } a \neq 0 \text{ ha grado } n \end{cases}$$
è una norma speciale su $\mathbf{Z}[x]$.
(4) Sia A un dominio dotato di una norma speciale N. Mostrate che la funzione $N' : A[x] \to \mathbf{N}$ data da
$$\begin{cases} N'(0) = 0 \\ N'(a) = N(a_n) \cdot 2^n & \text{se } a \neq 0 \text{ ha grado } n \end{cases}$$
è una norma speciale su $A[x]$.

Esercizio 11.17. Sia $A = \mathbf{Z}[i]$ il dominio degli *interi di Gauss*. Per $z \in \mathbf{C}$, sia $|\, z \,|$ il suo modulo.

Si mostri che la funzione

$$N : A \to \mathbf{N}$$
$$a_0 + ia_1 \mapsto |\, a_0 + ia_1 \,|^2 = a_0^2 + a_1^2,$$

per $a_0, a_1 \in \mathbf{Z}$, è una norma speciale su A, e si mostri che le unità di A sono $1, -1, i, -i$.