TRENTO, A.A. 2020/21
CORSO DI ALGEBRA B
FOGLIO DI ESERCIZI # 6

Esercizio 6.1. Sia E/F una estensione di campi. Sia $0 \neq \alpha \in E$ algebrico su F, e sia

$$a(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$$

il polinomio minimo di α su F.

(1) Si mostri che $a_0 \neq 0$.
(2) Si mostri che α^{-1} è algebrico su F, con polinomio minimo

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

Esercizio 6.2. Siano A, B anelli commutativi con unità, e

$$\begin{aligned} \bar{\cdot} : A &\to B \\ a &\mapsto \bar{a} \end{aligned}$$

un morfismo di anelli con unità.

Mostrate che la funzione

$$\begin{aligned} \varphi : A[x] &\to B[x] \\ a_0 + a_1 x + \cdots + a_n x^n &\mapsto \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_n}x^n \end{aligned}$$

è un morfismo di anelli.

Esercizio 6.3. Sia B/F una estensione del campo F. Si mostri che se il grado $|B : F|$ è finito, allora ogni elemento di B è algebrico su F.

Esercizio 6.4. Si dimostri il seguente Criterio di Eisenstein, in entrambi i modi illustrati a lezione.

Lemma (Criterio di Eisenstein). *Sia*

$$a = a_n x^n + \cdots + a_1 x + a_0 \in \mathbf{Z}[x],$$

tale che $\gcd(a_0, \dots, a_n) = 1$.

Supponiamo che esista un primo p tale che

(1) $p \mid a_i$ *per* $i = 0, \dots, n-1$,
(2) $\gcd(a_0, \dots, a_n) = 1$,
(3) p^2 *non divide* a_0.

Allora f è irriducibile in $\mathbf{Z}[x]$.

Esercizio 6.5. Si mostri che per un intero $n > 0$ sono equivalenti:

(1) n è primo, e
(2) n divide $\binom{n}{i}$ per ogni $0 < i < n$.

(Suggerimento: L'implicazione da (2) a (1) è facoltativa.)

Esercizio 6.6. Si mostri che per ogni primo p il polinomio

$$x^{p-1} + x^{p-2} + \cdots + x + 1$$

è irriducibile in $\mathbf{Z}[x]$.

(Suggerimento: Si può sare il successivo Esercizio 6.8.)

Esercizio 6.7.

(1) Sia E/F una estensione di campi. Si mostri che la somma e il prodotto di due elementi di E che siano algebrici su F sono ancora algebrici su F.
(2) Si trovi una estensione di $\mathbf{Q}$ che sia algebrica, di grado infinito.

Esercizio 6.8 (La prima parte è un caso particolare della seconda).

(1) Sia F un campo, $F[x], F[y]$ anelli di polinomi. Siano $a, b \in F$, con $a \neq 0$.
   Si mostri che esiste un unico morfismo di anelli $\varphi : F[x] \to F[y]$ tale che
   (a) $\varphi(c) = c$ per $c \in F$, e
   (b) $\varphi(x) = ay + b$,
   e che φ è un isomorfismo di anelli.
(2) Sia A un anello commutativo con unità, $A[x], A[y]$ anelli di polinomi. Siano $a, b \in A$, con a una unità.
   Si mostri che esiste un unico morfismo di anelli $\varphi : A[x] \to A[y]$ tale che
   (a) $\varphi(c) = c$ per $c \in A$, e
   (b) $\varphi(x) = ay + b$,
   e che φ è un isomorfismo di anelli.

Esercizio 6.9. Si mostri che l'insieme dei numeri algebrici (quando si parla di *numeri algebrici* senza precisare dove, si intende *i numeri complessi che siano algebrici su* $\mathbf{Q}$) è numerabile.

Esercizio 6.10 (Già discusso, ma vale come introduzione all'esercizio successivo).

(1) Si mostri che un campo è un dominio.
   (Suggerimento: Sia F un campo, e $a, b \in F$. Sia $ab = 0$. Se $a \neq 0$, allora a è invertibile, e dunque $0 = a^{-1} \cdot 0 = a^{-1} \cdot (ab) = b$.)
(2) Sia B un dominio, e A un sottoanello di B. Allora A è un dominio.
   (Suggerimento: Siano $x, y \in A$, e sia $xy = 0$. Dato che $A \subseteq B$, si ha $x, y \in B$. Dato che B è un dominio, si ha o $x = 0$, o $y = 0$.)
(3) Mettendo insieme le due cose precedenti, si ottiene che se E è un campo, se A è un suo sottoanello, allora A è un dominio. Di più non si può dire, dato che $\mathbf{Q}$ è un campo, $\mathbf{Z}$ è un sottoanello di $\mathbf{Q}$, e $\mathbf{Z}$ è un dominio, ma non un campo.
(4) Per il viceversa, si veda il prossimo esercizio.

Esercizio 6.11. Sia A un dominio. Si dia la costruzione del campo dei quozienti $Q(A)$ di A. In particolare

(1) Si mostri che la relazione su $A \times A^\star$ data da $(a, b)R(c, d)$ se e solo se $ad = bc$ è una relazione di equivalenza. (Qui $A^* = A \setminus \{ 0 \}$.)

(2) Sia $\dfrac{a}{b} = [(a, b)]$ la classe di $(a, b) \in A \times A^\star$ rispetto alla relazione R, e sia $Q(A) = \left\{ \dfrac{a}{b} : a \in A, b \in A^\star \right\}$ l'insieme delle classi di equivalenza.

(3) Si mostri che le operazioni su $Q(A)$.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

sono ben definite.

(4) (Facoltativa la dimostrazione) Si mostri che con queste operazioni $Q(A)$ diventa un anello commutativo.

(5) Si mostri che $\dfrac{0}{1}$ è lo zero di $Q(A)$, e $\dfrac{1}{1}$ ne è l'unità.

(6) Si mostri che la funzione $\iota : A \to Q(A)$ definita da $a \mapsto \dfrac{a}{1}$ è un morfismo iniettivo di anelli.

(7) Si mostri che $\dfrac{a}{b} \neq 0$ (si intende dunque $\dfrac{a}{b} \neq \dfrac{0}{1}$) se e solo se $a \neq 0$, e che in tal caso $\dfrac{a}{b}$ è invertibile, con inverso $\dfrac{b}{a}$. Se ne deduca che $Q(A)$ è un campo.

(8) Si mostri che $\dfrac{a}{b} = \dfrac{a}{1} \cdot \left(\dfrac{b}{1}\right)^{-1}$. Identificando $a \in A$ con la sua immagine $\iota(a) = \dfrac{a}{1}$ in $Q(A)$, si può dunque scrivere $\dfrac{a}{b} = a \cdot b^{-1}$.

(9) Sia F un campo, e $f : A \to F$ un morfismo iniettivo.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\iota"] & F \\ Q(A) \arrow[ur, dotted, "g"'] & \end{tikzcd}$$

Si mostri che esiste un'unico morfismo $g : Q(A) \to F$ che fa commutare il diagramma, e che esso è iniettivo.

Esercizio 6.12. Sia $f(x) \in F[x]$ un polinomio monico, non costante, ove F è un campo.

Si mostri che $[z] \in F[z]/(f(z))$ è radice del polinomio $f(x)$.