TRENTO, A.A. 2015/16
CORSO DI ALGEBRA
FOGLIO DI ESERCIZI # 9

Esercizio 9.1. Si consideri $\alpha = \sqrt{2} + \sqrt{3} \in \mathbf{C}$. Non è necessario dimostrare i punti seguenti nell'ordine indicato.

(1) Si trovi un polinomio monico $f \in \mathbf{Q}[x]$ di grado 4 di cui α è radice.
(2) Si mostri che $|\mathbf{Q}[\alpha] : \mathbf{Q}| \leq 4$.
(3) Si mostri che $\sqrt{2} \in \mathbf{Q}[\alpha]$.
(4) Si mostri che $F = \mathbf{Q}[\sqrt{2}] \subseteq \mathbf{Q}[\alpha]$.
(5) Si mostri che $\sqrt{3} \in \mathbf{Q}[\alpha]$.
(6) Si mostri che $F[\sqrt{3}] \subseteq \mathbf{Q}[\alpha]$.
(7) Si mostri che $|\mathbf{Q}[\sqrt{2}] : \mathbf{Q}| = 2$.
(8) Si mostri che $|F[\sqrt{3}] : F| = 2$.
(9) Si deduca dai due punti precedenti che $|F[\sqrt{3}] : \mathbf{Q}| = 4$.
(10) Si mostri che $F[\sqrt{3}] = \mathbf{Q}[\alpha]$.
(11) Si mostri che $|\mathbf{Q}[\alpha] : \mathbf{Q}| = 4$.
(12) Si mostri che f è il polinomio minimo di α su $\mathbf{Q}$.

Esercizio 9.2. Si consideri $\alpha = \sqrt{2} + \sqrt{3}$.

- Si mostri che α è radice del polinomio $f = x^4 - 10x^2 + 1 \in \mathbf{Q}[x]$.
- Si mostri che per ogni $\varepsilon, \eta \in \{ 1, -1 \}$ si ha che
$$\varepsilon\sqrt{2} + \eta\sqrt{3}$$
è radice di f,
- Se ne deduca che
$$\begin{aligned} f = &(x - (+\sqrt{2} + \sqrt{3}))\cdot \\ &(x - (-\sqrt{2} + \sqrt{3}))\cdot \\ &(x - (+\sqrt{2} - \sqrt{3}))\cdot \\ &(x - (-\sqrt{2} - \sqrt{3})). \end{aligned}$$
- Si mostri che $\varepsilon\sqrt{2} + \eta\sqrt{3} \notin \mathbf{Q}$ per ogni $\varepsilon, \eta \in \{ 1, -1 \}$.
- Sia ora m il polinomio minimo di α su $\mathbf{Q}$. Si spieghi perché m divide f.
- Si noti che in $\mathbf{R}[x]$ si ha che $x - \alpha$ divide m, dato che α è una radice di m.
- Si mostri che $f = m$. Per questo si faccia vedere che l'unico divisore monico $g \in \mathbf{Q}[x]$ di f che sia a sua volta divisibile per $x - \alpha$ è f stesso.

(Suggerimento: Per quel che riguarda l'ultima domanda, occorre distinguere le possibilità per il grado di g. Se grado$(g) = 1$, allora $g = x - \alpha$, e qui si usa uno dei punti precedenti. Se grado$(g) = 2$, allora $g = (x - \alpha)(x - \beta)$, ove β è una delle altre radici di f, dunque ci sono tre casi da considerare. Infine se grado$(g) = 3$, conviene notare che dato che $g \in \mathbf{Q}[x]$, e g divide f, deve essere $f = gh$ per un opportuno $h \in \mathbf{Q}[x]$ (monico) di grado 1, dunque h è un divisore di grado 1 di $f\dots$)

Esercizio 9.3. Siano $F \subseteq K \subseteq E$ sono campi, ognuno estensione di quelli più piccoli, e sia $\alpha \in E$, algebrico su F.

(1) Si mostri che il polinomio minimo di α su E è $x - \alpha$.
(2) Si mostri che α è algebrico anche su K.
(3) Detti m_F, m_k rispettivamente i polinomi minimi di α su F, K, si mostri che
$$x - \alpha \mid m_K \mid m_F.$$

Esercizio 9.4. Siano A, B anelli, $f : A \to B$ un morfismo. Si mostri che sono equivalenti:

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

Esercizio 9.5. Sia A un anello con unità.

(1) Si mostri che A e $\{ 0 \}$ sono ideali di A.
(2) Si mostri che se un ideale I di A contiene 1, allora $I = A$.
(3) Si mostri che se un ideale I di A contiene una unità, allora $I = A$.
(4) Si mostri che se A è un campo, allora gli unici ideali di A sono A e $\{ 0 \}$
(5) Si mostri che se A è un campo, e B un anello, e $f : A \to B$ è un morfismo, allora o $f(a) = 0$ per ogni $a \in A$, o f è iniettivo.

Esercizio 9.6. 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.
(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 9.7. Si enunci e si dimostri il Lemma di Eisenstein.

Esercizio 9.8. Sia n un intero positivo. Si mostri che sono equivalenti:

(1) n è un numero primo, e
(2) per ogni i, $0 < i < n$, si ha

$$n \text{ divide } \binom{n}{i}.$$

Esercizio 9.9. Sia A l'insieme degli elementi algebrici, cioè

$$A = \{ \alpha \in \mathbf{C} : \alpha \text{ è algebrico su } \mathbf{Q} \}.$$

(1) Si mostri che A è un campo.
(2) Si mostri che $|A : \mathbf{Q}|$ è infinito.
(3) Si mostri che A è numerabile.

Esercizio 9.10. Siano A, B anelli, e $\varphi : A \to B$ un isomorfismo.

(1) Si ricordi che $\varphi(0) = 0$, e $\varphi(1) = 1$,
(2) Si mostri che $\varphi^{-1} : B \to A$ è un isomorfismo.
(3) Supponiamo d'ora in poi che A, B siano domini.
(4) Si mostri che se $a \in A$ è una unità, allora anche $\varphi(a) \in B$ è una unità. (Per il punto (2), si tratta dunque di un "se e solo se", e questo vale anche per i punti seguenti.)
(5) Si mostri che se $a_1, a_2 \in A$ sono associati, allora $\varphi(a_1), \varphi(a_2) \in B$ sono associati.
(6) Si mostri che se $a \in A$ è irriducibile, allora $\varphi(a) \in B$ è irriducibile.
(7) Si mostri che se $a \in A$ è primo, allora $\varphi(a) \in B$ è primo.

Esercizio 9.11. Sia $a \in \{ +1, -1 \}$, e $b \in \mathbf{Z}$.

Siano $\mathbf{Z}[x], \mathbf{Z}[y]$ due anelli di polinomi. Si mostri che esiste un unico morfismo

$$\varphi : \ \mathbf{Z}[x] \to \mathbf{Z}[y]$$

tale che

$$\lambda \mapsto \lambda, \text{ per } \lambda \in \mathbf{Z}$$
$$x \mapsto ay + b$$

e che tale φ è un isomorfismo di anelli. Per quest'ultimo punto, si dica esplictamente chi è $\varphi^{-1} : \mathbf{Z}[y] \to \mathbf{Z}[x]$.

Esercizio 9.12.

(1) Si mostri che per ogni numero primo p il polinomio
$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$
è irriducibile in $\mathbf{Z}[x]$;

(2) Si mostri che per ogni numero primo *dispari* p, il polinomio
$$\frac{x^p + 1}{x + 1} = x^{p-1} - x^{p-2} + \cdots + (-1)^i x^i + \cdots - x + 1$$
è irriducibile in $\mathbf{Z}[x]$. (**Notate** che per $p = 2$, si ha che $x + 1$ non divide $x^2 + 1$.)