Andrea Gadotti

Esercizio 1

Vogliamo esprimere $(\alpha^2+\alpha+1)(\alpha^2+\alpha)$ e $(\alpha-1)^{-1}$ nella forma

$$a\alpha^2+b\alpha+c$$

Poiché $\alpha^3+\alpha^2+\alpha+2=0$, si ha $\alpha^3=-\alpha^2-\alpha-2$, e quindi $\alpha^4=\alpha\alpha^3=-\alpha^3-\alpha^2-2\alpha=-\alpha+2$. Allora:

$$(\alpha^2+\alpha+1)(\alpha^2+\alpha)=\alpha^4+2\alpha^3+2\alpha^2+\alpha=-2\alpha-2$$

Quindi $a=0, b=-2, c=-2$.
Consideriamo ora $\beta:=(\alpha-1)^{-1}$. β è tale che $(\alpha-1)\beta=1$, ovvero $(a\alpha^2+b\alpha+c)(\alpha-1)=1$. Sviluppando il prodotto si trova:

$$(b-2a)\alpha^2+(c-a-b)\alpha-(2a+c)=1$$

Abbiamo quindi il seguente sistema:

$$\begin{cases} b-2a=0 \\ c-a-b=0 \\ 2a+c=0 \end{cases}$$

Si trova facilmente che il sistema ha soluzione $a=-\frac{1}{5}, b=-\frac{2}{5}, c=-\frac{3}{5}$.

Esercizio 2

Supponiamo $[F(\alpha):F]=2n+1$ per qualche $n\in\mathbb{N}$. Allora:

$$[F(\alpha):F(\alpha^2)][F(\alpha^2):F]=[F(\alpha):F]=2n+1$$

quindi entrambi i fattori del prodotto sono dispari. Affermiamo che $[F(\alpha):F(\alpha^2)]=1$ (e quindi $F(\alpha)=F(\alpha^2)$). Osserviamo che il polinomio $x^2-\alpha^2\in F(\alpha^2)[x]$ ha banalmente α come radice, quindi $[F(\alpha):F(\alpha^2)]$ è 1 o 2. Ma 2 non è dispari, quindi $[F(\alpha):F(\alpha^2)]=1$.

Esercizio 3

Abbiamo

$$[F(\alpha,\beta):F(\alpha)][F(\alpha):F]=[F(\alpha,\beta):F]=[F(\alpha,\beta):F(\beta)][F(\beta):F]$$

ovvero

$$[F(\alpha,\beta):F(\alpha)]\cdot\deg(f)=[F(\alpha,\beta):F(\beta)]\cdot\deg(g)$$

Quindi $\deg(g)\,|\,[F(\alpha,\beta):F(\alpha)]\cdot\deg(f)$. Poiché $\deg(f)$ e $\deg(g)$ sono coprimi per ipotesi, si ha $\deg(g)\,|\,[F(\alpha,\beta):F(\alpha)]$. Ma ovviamente $[F(\alpha)(\beta):F(\alpha)]\leq[F(\beta):F]=\deg(g)$, quindi $[F(\alpha,\beta):F(\alpha)]=\deg(g)$, ovvero g è irriducibile su $F(\alpha)$.

Esercizio 4

Sia $\alpha:=\sqrt[4]{2}$. Il suo polinomio minimo su $\mathbb{Q}$ è banalmente x^4-2, quindi $|\ \mathbb{Q}(\alpha):\mathbb{Q}\ |=4$. Stiamo cercando i campi intermedi. Supponiamo allora di avere $\beta\in\mathbb{Q}(\alpha)$ con $\beta\notin\mathbb{Q}$. Poiché

$$|\ \mathbb{Q}(\alpha)(\beta):\mathbb{Q}(\beta)\ |\cdot|\ \mathbb{Q}(\beta):\mathbb{Q}\ |=4$$

è chiaro che dobbiamo avere $|\ \mathbb{Q}(\beta):\mathbb{Q}\ |=2$.
Consideriamo allora il polinomio minimo di β su $\mathbb{Q}$. Esso dovrà essere della forma $x^2+\gamma+\delta$. Supponiamo β e β' radici. Allora $\beta+\beta'=\gamma\in\mathbb{Q}$ e $\beta\beta'=\delta\in\mathbb{Q}$. Poiché

$$\mathbb{Q}(\sqrt[4]{2})=\{a+b\alpha+c\alpha^2+d\alpha^3\mid\alpha^4=2,\ a,b,c,d\in\mathbb{Q}\}$$

si ha che

$$\beta=a+b\alpha+c\alpha^2+d\alpha^3,\ \ \beta'=a'+b'\alpha+c'\alpha^2+d'\alpha^3$$

dove i coefficienti stanno in $\mathbb{Q}$. Poiché $\beta+\beta'\in\mathbb{Q}$, si ha banalmente $b=-b',c=-c',d=-d'$. Quindi

$$\beta=a+\xi\alpha,\ \ \beta'=a'-\xi\alpha,\ \ \text{con }\xi:=b+c\alpha+d\alpha^2$$

Osservando che $\beta\beta'=(a+\xi\alpha)(a'-\xi\alpha)\in\mathbb{Q}$ e facendo i conti si trova facilmente che $b=0$ e $d=0$. Ovvero $\beta=a+c\alpha^2$, ovvero $Q(\beta)=\mathbb{Q}(\sqrt{2})$.

Esercizio 5

Sia $f(x)=x^6+x^3+1\in\mathbb{Q}[x]$. Osserviamo che $(x^3-1)f(x)=x^9-1$, quindi le radici di f in $\mathbb{C}$ sono le radici none dell'unità che non sono anche radici terze.

Quindi, poiché $\sigma(\alpha)$ deve essere ancora una radice di f (e l'omomorfismo è completamente determinato da essa), abbiamo che gli omomorfismi cercati sono 6 e sono dati da:

$$\sigma_k(\alpha) := e^{2\pi ik/9}$$

dove $k = 1, 2, 4, 5, 7, 8$.

Esercizio 6

$\sqrt{2}+\sqrt{3}$ è algebrico su $\mathbb{Q}$, di grado 4. Infatti $\sqrt{2}+\sqrt{3}$ è radice del polinomio

$$x^4 - 10x^2 + 1$$

Rimane da mostrare che $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$. Osserviamo innanzitutto che $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$. Questo si mostra facilmente con la formula dei gradi, in quanto è semplice far vedere che $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.
Ma allora, per la formula dei gradi, abbiamo che

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2}+\sqrt{3})][\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$$

Mostriamo che $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2}+\sqrt{3})] = 1$. Infatti $(\sqrt{2}+\sqrt{3})^3 = 11\sqrt{2}+9\sqrt{3}$, quindi

$$\frac{(\sqrt{2}+\sqrt{3})^3 - 9(\sqrt{2}+\sqrt{3})}{2} = \sqrt{2}$$

Quindi $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2}+\sqrt{3})] = 1$ e perciò $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$.

Esercizio 7

Sappiamo che qualsiasi estensione di grado finito è un'estensione algebrica. Poiché E e F hanno grado finito, abbiamo che $E = k(\alpha_1, ..., \alpha_n)$ e $F = k(\beta_1, ..., \beta_m)$. Quindi $EF = k(\alpha_1, ..., \alpha_n, \beta_1, ..., \beta_m)$. Per la formula dei gradi, sappiamo che

$$[EF : k] = [EF : F][F : k]$$

Poiché ogni polinomio in $k[x]$ è anche un polinomio in $F[x]$, è chiaro che $[EF : F] \leq [E : k]$, ovvero

$$[EF : k] \leq [E : k][F : k]$$

Mostriamo che se $[E : k]$ e $[F : k]$ sono coprimi, allora vale l'uguaglianza. Ricordiamo che $E = k(\alpha_1, ..., \alpha_n)$. Procediamo per induzione su n:

- Se $n = 0$, allora significa che $EF = F$, quindi la tesi è banalmente soddisfatta.

- Se $n > 0$, supponiamo $[k(\alpha_1, ..., \alpha_n)F : F] < [k(\alpha_1, ..., \alpha_n) : k]$. Per la formula dei gradi,

  $$[k(\alpha_1, ..., \alpha_n)F : F] = [(k(\alpha_1, ..., \alpha_{n-1})F)(\alpha_n) : k(\alpha_1, ..., \alpha_{n-1})F][k(\alpha_1, ..., \alpha_{n-1})F : kF]$$

  e

  $$[k(\alpha_1, ..., \alpha_n) : k] = [k(\alpha_1, ..., \alpha_{n-1})(\alpha_n) : k(\alpha_1, ..., \alpha_{n-1})][k(\alpha_1, ..., \alpha_{n-1}) : k]$$

  Poiché per ipotesi il primo termine è strettamente minore del secondo, significa che

  (a) $[k(\alpha_1, ..., \alpha_{n-1})F : kF] < [k(\alpha_1, ..., \alpha_{n-1}) : k]$, oppure

  (b) $[(k(\alpha_1, ..., \alpha_{n-1})F)(\alpha_n) : k(\alpha_1, ..., \alpha_{n-1})F] < [k(\alpha_1, ..., \alpha_{n-1})(\alpha_n) : k(\alpha_1, ..., \alpha_{n-1})]$

  Se vale (a), per ipotesi induttiva significa che $[k(\alpha_1, ..., \alpha_{n-1}) : k]$ e $[F : k]$ non sono coprimi. Ma allora neanche $[E : k] = [k(\alpha_1, ..., \alpha_{n-1})(\alpha_n) : k(\alpha_1, ..., \alpha_{n-1})][k(\alpha_1, ..., \alpha_{n-1}) : k]$ e $[F : k]$ sono coprimi, e quindi la dimostrazione è conclusa.
  Se non vale (a), allora deve valere (b). Ma allora possiamo proseguire "estraendo" ogni volta un α_j, e prima o poi dovremo necessariamente giungere a una situazione sostanzialmente uguale ad (a).

Esercizio 8

Procediamo per induzione su n. Se $n = 1$ la tesi è banalmente vera. Supponiamo ora che sia vero per ogni numero $\leq n$ e mostriamo che vale anche per $n + 1$. Sia allora F un campo e sia $f(x) \in F[x]$ un polinomio di grado $n + 1$. Sia K il campo di spezzamento di f.

- Se $f(x)$ è riducibile, sia $p(x) \in F[x]$ un suo fattore irriducibile (quindi $1 \leq \deg p \leq n$). Sia E il campo di spezzamento di $p(x)$. Allora $f(x) = p(x)g(x)$ per qualche $g(x) \in E[x]$. Abbiamo allora che K è il campo di spezzamento di $g(x)$ su E. Per ipotesi induttiva, otteniamo $[E : F] \mid (\deg p)!$ e $[K : E] \mid (\deg g)!$. Per la formula dei gradi sappiamo che $[K : F] = [K : E][E : F]$. Quindi

  $$[K : F] \mid (\deg p)!\,(\deg g)!$$

  Ma poiché $\forall a, b \in \mathbb{N}$ vale $a!\,b! \mid (a+b)!$, abbiamo che $[K : F] \mid (\deg p + \deg g)! = (\deg f)!$ e la tesi è provata.

- Se $f(x)$ è irriducibile, sia α una sua radice. Chiaramente $[F(\alpha) : F] = n+1$ e $f(x) = (x-\alpha)g(x)$ con $g(x) \in F(\alpha)$ che ha grado n. Quindi K è il campo di spezzamento di $g(x)$ su $F(\alpha)$ e allora per ipotesi induttiva $[K : F(\alpha)] \mid n!$. Per la formula dei gradi vale
$$[K : F] = [K : F(\alpha)][F(\alpha) : F]$$
e perciò $[K : F] \mid (n+1)n! = (n+1)!$.

Esercizio 9

Sia $f(x) = x^{p^8} - 1 \in \mathbb{Z}/p\mathbb{Z}[x]$ con p primo. Allora $f(x) = (x-1)^{p^8}$, quindi l'unica radice di $f(x)$ è 1. Perciò in campo di spezzamento di f è $\mathbb{Z}/p\mathbb{Z}[x]$ stesso.

Esercizio 10

Sia $\alpha \in \mathbb{R}$ tale che $\alpha^4 = 5$.

(a) È chiaro che $\alpha^2 = \sqrt{5}$. Vogliamo mostrare che $\mathbb{Q}(i\alpha^2) = \mathbb{Q}(i\sqrt{5})$ è estensione normale di $\mathbb{Q}$. Sia $f(x) = x^2 + 5$. Le radici di f sono $\pm i\sqrt{5} \in \mathbb{Q}(i\sqrt{5})$, che quindi è il campo di spezzamento per il polinomio f.

(b) Osserviamo che $(\alpha + i\alpha)^2 = \alpha^2 + 2i\alpha^2 - \alpha^2 = 2i\alpha^2 \in \mathbb{Q}(i\alpha^2)$. Quindi $\mathbb{Q}(\alpha + i\alpha)$ è il campo di spezzamento per il polinomio $f(x) = x^2 - 2i\alpha^2 \in \mathbb{Q}(i\alpha^2)$.

(c) Osserviamo che $\alpha + i\alpha$ è radice del polinomio $f(x) = x^4 + 20 \in \mathbb{Q}[x]$. Inoltre f è irriducibile, in quanto in $\mathbb{C}$ abbiamo che
$$f(x) = (x-\beta_1)(x-\beta_2)(x-\beta_3)(x-\beta_4)$$
dove $\beta_1 = \alpha + i\alpha, \beta_2 = -\alpha + i\alpha, \beta_3 = -\alpha - i\alpha, \beta_4 = \alpha - i\alpha$, e nessuno dei fattori sta in $Q[x]$ e nemmeno nessun prodotto di due fattori.
Ci basta quindi mostrare che esiste una radice di f che non sta in $\mathbb{Q}(\alpha + i\alpha)$. Supponiamo per assurdo che $\beta_1, \beta_4 \in \mathbb{Q}(\alpha + i\alpha)$. Allora anche $\alpha = \beta_1 - \beta_4 \in \mathbb{Q}(\alpha + i\alpha)$, e quindi anche $i = \beta_1\alpha^{-1} \in \mathbb{Q}(\alpha + i\alpha)$. Quindi $\mathbb{Q}(\alpha, i) \subseteq \mathbb{Q}(\alpha + i\alpha)$. Ma $\mathbb{Q}(\alpha + i\alpha)$ ha grado 4 su $\mathbb{Q}$, mentre è facile vedere che $\mathbb{Q}(\alpha, i)$ ha grado 8 su $\mathbb{Q}$ (si usa la formula dei gradi e il fatto immediato che $\sqrt[4]{5} \notin \mathbb{Q}(i)$).

Esercizio 11

(c) Su $\mathbb{C}$, $f(x) = (x-\alpha)(x-\alpha_2)(x-\alpha_3)$ dove $\alpha = \sqrt[3]{2}$, $\alpha_2 = \alpha(-1/2 + i\sqrt{3}/2)$, $\alpha_3 = \alpha(-1/2 - i\sqrt{3}/2)$. Quindi il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ è $\mathbb{Q}(\alpha, \alpha_2, \alpha_3)$. Osserviamo che $\alpha_3 = -\alpha - \alpha_2$, quindi $\mathbb{Q}(\alpha, \alpha_2, \alpha_3) = \mathbb{Q}(\alpha, \alpha_2)$. Quindi, preso $\varepsilon := i\sqrt{3}$, abbiamo banalmente $\mathbb{Q}(\alpha, \alpha_2) = \mathbb{Q}(\alpha, \varepsilon)$. Affermo che $[\mathbb{Q}(\alpha, \varepsilon) : \mathbb{Q}] = 6$, e questo chiaro usando l'Esercizio 7 e il fatto che $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ e $[\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}] = 2$.

Esercizio 12

Vogliamo mostrare che in K valgono $\forall y \exists x (y = x^p)$ e $\forall a, b (a^p = b^p \Rightarrow a = b)$. Il secondo punto è immediato, perché $a^p - b^p = 0 \Rightarrow (a-b)^p = 0 \Rightarrow a - b = 0 \Rightarrow a = b$. Mostriamo il primo punto: se $y = 0$ è banale. Se $y \neq 0$, poiché K è un campo con p^n elementi, si ha che $|K^*| = p^n - 1$. Quindi $y^{p^n-1} = 1$, ovvero $y^{p^n} = y$. Osserviamo adesso che, preso $y^{p^{n-1}} \in K$, si ha

$$\left(y^{p^{n-1}}\right)^p = y^{p^n} = y$$

ovvero $y^{p^{n-1}}$ è la radice p-sima cercata.

Esercizio 13

Sia L il campo di spezzamento di $f(x) \in K[x]$. Sia A l'insieme di tutte le radici di f, che per ipotesi sono distinte e formano un campo. A è quindi un campo finito, ovvero $|A| = p^n$ per qualche $n \geq 1$, dove $p = \operatorname{char} A$. Quindi $\deg f = p^n$. Osserviamo che

$$g(x) := x^{p^n} - x \in K[x]$$

ha come radici proprio l'insieme A. Infatti $x^{p^n} - x = x(x^{p^n-1} - 1)$. Quindi g ha come radici 0 e tutti gli x tali che $x^{p^n-1} = 1$. Ma quest'ultima equazione è soddisfatta da qualsiasi elemento di A^*. Ne segue banalmente che $f = g$.
Poiché A è un campo contenuto in L, si ha che $\operatorname{char} L = \operatorname{char} A = p = \operatorname{char} K$.

Esercizio 14

Sappiamo che se $\operatorname{char} K = p$ e $L \supseteq K$ con $[L : K] < \infty$, allora

$$[L : K] = p^m \, [L : K]_S$$

con $m \in \mathbb{N}$. Quindi, poiché $[L : K]$ e p sono coprimi per ipotesi, abbiamo che $m = 0$, ovvero $[L : K] = [L : K]_S = [L \cap K^S : K]$. E poiché $L \cap K^S \subseteq L$, si ha $L \cap K^S = L$. Quindi ogni elemento di L è separabile su K.

Esercizio 15

Osserviamo che

$$f(x) := x^{p^n} - a = x^{p^n} - \alpha^{p^n} = (x - \alpha)^{p^n}$$

dove α è una radice p^n-esima di a in qualche estensione di K.
Sia $(x - \alpha)^r$ un fattore irriducibile di f in $K[x]$. Possiamo scrivere $r = sp^m$ con $m \leq n$ e s coprimo con p. Allora

$$(x - \alpha)^r = (x - \alpha)^{sp^m} = (x^{p^m} - \alpha^{p^m})^s = x^{sp^m} - s\alpha^{p^m} x^{(s-1)p^m} + \dots$$

Quindi $s\alpha^{p^m} \in K$, e poiché in K vale $s \neq 0$, s è invertibile e perciò $\alpha^{p^m} \in K$. Quindi $(\alpha^{p^m})^{p^{n-m-1}} \in K$ è una radice p-esima di a, il che contraddice l'ipotesi.

Esercizio 16

Proviamo "$\Longrightarrow$". Sia $x^{p^n} - \alpha^{p^n} \in K(\alpha^{p^n})[x]$. Se per assurdo fosse irriducibile, allora esso sarebbe il polinomio minimo di α. Ma su $K(\alpha)[x]$ vale $x^{p^n} - \alpha^{p^n} = (x - \alpha)^{p^n}$, ovvero α è una radice multipla del suo polinomio minimo, il che è impossibile perché α è separabile per ipotesi. Quindi $x^{p^n} - \alpha^{p^n}$ è riducibile, perciò grazie all'Esercizio 15 abbiamo che $K(\alpha^{p^n})$ contiene una radice p-esima di α^{p^n}. La radice in questione è proprio $\alpha^{p^{n-1}}$, in quanto l'endomorfismo di Frobenius è iniettivo.
Quindi su $K(\alpha^{p^n}) = K(\alpha^{p^{n-1}})$, e poiché quanto provato vale per ogni n, si ha la tesi.

Proviamo "$\Longleftarrow$". Sia $f(x) \in K[x]$ il polinomio minimo di α. Poiché f è irriducibile, sappiamo che $f(x) = g(x^{p^r})$ per qualche $r \in \mathbb{N}$, dove $g(y)$ è un polinomio in $K[x]$ irriducibile e separabile. Osserviamo che $g(\alpha^{p^r}) = f(\alpha) = 0$, ovvero α^{p^r} è radice di g, ovvero α^{p^r} è separabile su K. Quindi $K(\alpha^{p^r})$ è un'estensione separabile di K. Ma $K(\alpha^{p^r}) = K(\alpha)$ per ipotesi, perciò la dimostrazione è conclusa.

Esercizio 17

Proviamo $(a) \Longrightarrow (b)$. Supponiamo per assurdo che esista $a \in K$ che non ha una radice p-esima in K. Consideriamo il polinomio $x^p - a$ e sia α una sua radice.

Nel suo campo di spezzamento, abbiamo che

$$x^p - a = x^p - \alpha^p = (x - \alpha)^p$$

Questo significa che il polinomio minimo di α su K divide $(x - \alpha)^p$, ovvero il polinomio in questione ha radici multiple, ovvero $K(\alpha)$ non è separabile, e questo contraddice l'ipotesi.
Proviamo $(b) \implies (a)$. Supponiamo per assurdo che esista un α algebrico su K il cui polinomio minimo f possiede radici multiple (possiamo anche supporre senza perdità di generalità che α sia proprio una radice multipla del suo polinomio minimo). Sappiamo che questo significa che $\operatorname{char} K = p > 0$ e che f è della forma

$$f = x^{pn} + a_{n-1}x^{p(n-1)} + \cdots + a_1x^p + a_0$$

Per ipotesi, possiamo trovare $b_0, ..., b_{n-1}$ tali che

$$f = x^{pn} + b_{n-1}^p x^{p(n-1)} + \cdots + b_1^p x^p + b_0^p$$

ovvero

$$f = (x^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0)^p$$

Poiché $f(\alpha) = 0$, allora anche $(\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0)^p = 0$, e poiché l'endomorfismo di Frobenius è iniettivo, questo significa che $\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0$, ovvero

$$x^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0 \in K[x]$$

ha α come radice ed ha grado strettamente minore di f, quindi abbiamo una contraddizione.

Esercizio 18

Vogliamo dimostrare che se K è un campo finito, allora $\forall x \in K,\ x = a^2 + b^2$ per qualche $a, b \in K$.

- Se $\operatorname{char} K = 2$, allora $x^{2n-1} = 1$, ovvero $x = x^{2n} = (x^n)^2$. Quindi $x = (x^n)^2 + 0^2$.
- Se $\operatorname{char} K = p > 2$, consideriamo il sottogruppo moltiplicativo K^*. K^* è un gruppo di ordine $p^n - 1$ per qualche n ed è ciclico. Quindi gli elementi che si possono scrivere come quadrati sono almeno tutte le potenze pari del generatore di K^*, ovvero sono almeno $(p^n - 1)/2$. Poiché $0 = 0^2$, i quadrati in K sono almeno $(p^n + 1)/2$. Quindi, se $A := \{y \in K \mid y = a^2 \text{ per qualche } a \in K\}$

e $X := \{x \in K \mid x = a^2 + b^2 \text{ per qualche } a, b \in K\}$, abbiamo che $X = A + A$. Si vede facilmente che se S è un sottoinsieme di un gruppo finito G, e vale $|S| + |S| > |G|$, allora $G = S + S$. Poiché $|A| + |A| = p^n + 1 > p^n = |K|$, si ha che $K = A + A = X$.

Esercizio 19

Sia $E \subseteq R \subseteq F$ un sottoanello di E. Sia $\alpha \in R$. È sufficiente mostrare che $\alpha^{-1} \in R$. Osserviamo che, poiché α è algebrico su F, esiste $f(x) = \sum_{i=0}^{n} a_i x^i$ irriducibile tale che $f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i = 0$ ($a_0 \neq 0$ perché $f(x)$ è irriducibile).
Quindi $\alpha(-\sum_{i=1}^{n} a_i/a_0\ \alpha^{i-1}) = 1$ dove $-\sum_{i=1}^{n} a_i/a_0\ \alpha^{i-1} \in R$, e si ha la tesi.
Mostriamo che l'ipotesi di algebricità per E è necessaria, esibendo un controesempio: sia $F = \mathbb{Q}$ e sia $E = \mathbb{Q}(\pi)$. Sia R il più piccolo anello contenente Q e π. È chiaro che

$$R = \left\{ \sum_{i=1}^{n} c_i \pi^i \ \mid \ c_i \in \mathbb{Q},\ n \in \mathbb{N} \right\}$$

e quindi $\frac{1}{\pi} \notin R$.

Esercizio 20

a) Sia $y \in K$. Poiché $y \in F(x)$, si ha che $y = \frac{f(x)}{g(x)}$ per qualche $f, g \in F[t]$. È chiaro che $f(t) - g(t)y = f(t) - g(t)\frac{f(x)}{g(x)} \in K[t]$ ha x come radice.

b) Sia $p(t) = f(t) - g(t)y = f(t) - g(t)\frac{f(x)}{g(x)} \in F(y)[t]$. È chiaro che $p(t)$ ha x come radice e $\deg p = \max(\deg f, \deg g)$. Vogliamo mostrare che $p(t)$ è irriducibile. Iniziamo enunciando il seguente:

Lemma 0.0.1. Siano $f, g \in F[t]$ coprimi. Siano $P_n \in F[t]$ polinomi di grado strettamente minore di $m := \max(\deg(f), \deg(g))$. Se

$$\sum_{n=0}^{N} P_n f^n g^{N-n} = 0$$

per qualche $N \in \mathbb{N}$, allora $P_n = 0$ per ogni n.

Dimostrazione. Assumiamo senza perdità di generalità che $\deg(g) = m$. Allora g divide $\sum_{n=0}^{N-1} P_n f^n g^{N-n}$, perciò divide anche $P_N f^N$. Per coprimalità, abbiamo che g divide P_N, Ma dall'ipotesi sul grado dei P_n segue che $P_N = 0$. Otteniamo quindi che $\sum_{n=0}^{N-1} P_n f^n g^{(N-1)-n} = 0$ e si prosegue per induzione. $\square$

Sia ora $y = \frac{f(x)}{g(x)}$, con f e g coprimi in $F[t]$. Vogliamo mostrare che il polinomio minimo di x in $F(y)$ ha grado $m = \max(\deg(f), \deg(g))$. Sia p un polinomio in $F(y)[t]$, tale che $p(x) = 0$. Scriviamo $p(t) = \sum_{k=0}^{r} a_k t^k$, con $a_k \in F(y)$ e supponiamo $r < m$. Possiamo scrivere $a_k = \frac{P_k(y)}{Q_k(y)}$, con $P_k, Q_k \in F[t]$. Vale allora

$$\sum_{k=0}^{r} \frac{P_k(y)}{Q_k(y)} x^k = 0$$

Quindi otteniamo

$$\sum_{k=0}^{r} P_k(y) \prod_{k' \neq k} Q_{k'}(y) x^k = 0,$$

che riscriviamo come

$$\sum_{k=0}^{r} \widetilde{P_k(y)} x^k = 0,$$

dove $\widetilde{P_k} := P_k(y) \prod_{k' \neq k} Q_{k'}(y)$.

Se definiamo adesso $\widetilde{P_k} =: \sum_l a_{kl} t^l \in F[t]$, otteniamo

$$\sum_{k=0}^{r} \sum_{l} a_{kl} \frac{f(x)^l}{g(x)^l} x^k = 0.$$

Moltiplichiamo ora tutto per $g(x)^L$ con L abbastanza grande. Troviamo

$$\sum_{k=0}^{r} \sum_{l} a_{kl} f(x)^l g(x)^{L-l} x^k = 0,$$

Che possiamo riscrivere come

$$\sum_{l} (\sum_{k=0}^{r} a_{kl} x^k) f(x)^l g(x)^{L-l} = 0.$$

Grazie al lemma (e alla trascendenza di x), tutti gli a_{kl} sono 0. Quindi anche gli $\widetilde{P_k}$ sono 0 e si vede subito che anche tutti gli a_k sono 0. In conclusione, p è il polinomio nullo, e questo conclude la dimostrazione.