Lista 1.

1. Sea E/F una extensión de campos. Pruebe que

   a) $[E : F] = 1$ si, y sólo si $E = F$;

   b) Si $[E : F]$ es un número primo, entonces no existen subcampos intermedios en la extensión E/F, salvo los triviales;

   c) Si $\alpha \in E$ tiene grado n sobre F, entonces n divide a $[E : F]$.

   a) De una extensión de campos que no sea finita;

   b) De un ejemplo de un campo con un número finito de elementos.

Dem.

De a):

$\Leftarrow$) Suponga que $E = F$. Afirmamos que:

$$E = \mathcal{L}_F(1)$$

(siendo E y F no triviales). En efecto, sea $\alpha \in E$, ent. $\alpha \in F$, luego

$$\alpha = 1\cdot\alpha \in \mathcal{L}_F(1)$$

Luego $E = \mathcal{L}_F(1)$. Como $\{1\}$ es un conjunto l.i, ent. $[E:F] = |\{1\}| = 1$.

$\Rightarrow$) Suponga que $[E:F] = 1$. Ent. por ser E/F una extensión de campos, $F \subseteq E$. Probaremos que $E \subseteq F$.

Como $[E:F] = 1$, existe $\{\alpha\} \subseteq E \ni E = \mathcal{L}_F\{\alpha\}$. Probaremos que $\alpha \in F$. En efecto, sea $x \in F \subseteq E$, ent. $\exists\, y \in F \ni$ (con $x \neq 0$): $x = y\alpha$. Como $x \neq 0 \Rightarrow y \neq 0 \neq \alpha$. Por ende

$$F \ni xy^{-1} = \alpha$$

por ser F campo. Luego $\alpha \in F$. Sea $e \in E$, ent. $\exists\, f \in F \ni$

$$e = f\alpha \in F$$

pues $f, \alpha \in F$. Por tanto $E = F$.

De b): Sea K un campo $\ni$ $F \subseteq K \subseteq E$. Probaremos que $K = F$ o $K = E$. Por ser los tres campos:

$$[E:F] = [E:K]\cdot[K:F]$$

donde $[E:F] = p \in \mathbb{N}$ primo, en part. $[E:F] < \infty \Rightarrow [E:K], [K:F] < \infty$. Luego

$$[E:K]\cdot[K:F] = p$$

por ser p primo, debe suceder que $[K:F] = 1$ o $[E:K] = 1$. Por a) $\Rightarrow K = F$ o $K = E$.

De d): Considere la extensión $\mathbb{Q}(S)/\mathbb{Q}$, dónde

$$S = \{ \sqrt{p} \mid p \in \mathbb{N} \text{ es número primo} \}$$

Sea $n \in \mathbb{N}$. En un ejercicio, se probó que

$$[\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$$

donde $\{p_i\}_{i=1}^{\infty}$ es una enumeración de los números primos ascendente (siendo todos distintos). Ent.

$$[\mathbb{Q}(S) : \mathbb{Q}] = [\mathbb{Q}(S) : \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})] \cdot [\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) : \mathbb{Q}]$$

donde $[\mathbb{Q}(S) : \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})] \geq 1$, así:

$$\Rightarrow [\mathbb{Q}(S) : \mathbb{Q}] \geq 2^n > n$$

Luego, como el n fue arbitrario, ent. $[\mathbb{Q}(S) : \mathbb{Q}] = \infty$.

De e): $\mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2$.

De c): Como $\alpha \in E$ tiene grado n sobre F, ent. $[F(\alpha) : F] = n$ (donde $\alpha \in E$ es algebraico sobre F), entonces:

$$[E : F] = [E : F(\alpha)] \cdot [F(\alpha) : F]$$

$$\Rightarrow n\,[E : F(\alpha)] = [E : F]$$

Si $[E:F]$ o $[E : F(\alpha)]$ son finitos, ent. se sigue que $n \mid [E:F]$.

$\square$

2. Sean E/F una extensión de campos y $\alpha_1, \ldots, \alpha_n \in E$. Pruebe que $F(\alpha_1, \ldots, \alpha_n)$ es isomorfo al campo de cocientes del anillo $F[\alpha_1, \ldots, \alpha_n]$.

Dem.

Por un teorema, los elementos del anillo $F[\alpha_1, \ldots, \alpha_n]$ están caracterizados como sigue:

$$F[\alpha_1, \ldots, \alpha_n] = \{ f(\alpha_1, \ldots, \alpha_n) \mid f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n] \}$$

ent. su campo de cocientes será:

$$\operatorname{Coc}(F[\alpha_1, \ldots, \alpha_n]) = \left\{ \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} \;\middle|\; f(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n] \mid g(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}$$
$$= F(\alpha_1, \ldots, \alpha_n)$$

(por un teorema).

$\square$

3. Sean F y E subcampos del campo L. ¿Cuándo se cumple que $EF = F \cup E$?

4. Sean $E_1, \ldots, E_n$ subcampos de un campo E. Pruebe que

Sol.

Por def. se tiene que $EF = (E \cup F) = (F \cup E)$. Ent. si se cumple

$$(F \cup E) = F \cup E$$

$F \cup E$ debe ser un campo. Afirmamos que se da la igualdad ssi $E \subseteq F$ o $F \subseteq E$. En efecto, la suficiencia es necesaria, i.e $E \subseteq F$ o $F \subseteq E \Rightarrow EF = F \cup E$.

Suponga que $F \nsubseteq E$ y $E \nsubseteq F$, ent. $\exists$ $f \in F$ m $f \notin E$ y $e \in E$ m $e \notin F$. El elemento

$$ef \notin E \text{ y } ef \notin F$$

(tanto $e, f \neq 0$), pues si $ef \in E \Rightarrow \exists$ $e_1 \in E$ m $ef = e_1 \Rightarrow f = e_1 e^{-1} \in E$ $\nRightarrow\!\!\Leftarrow$, pues $f \notin E$ (de forma análoga con F). Luego

$$ef \notin E \cup F$$

Como $(E \cup F)$ es campo, ent $ef \in (E \cup F) \Rightarrow E \cup F \subsetneq (E \cup F) = EF$.

Así

$$EF = (E \cup F) \Leftrightarrow E \subseteq F \text{ o } F \subseteq E$$

$\square$

4. Sean $E_1, \dots, E_n$ subcampos de un campo E. Pruebe que

$$E_1 \cdots E_n = E_1(E_2(\cdots(E_{n-1}(E_n)))).$$

Dem.

Procederemos por inducción sobre n. Para $n=2$ el resultado es inmediato. Suponga se cumple para $n=K$. Probaremos que se cumple para $n=K+1$. En efecto, se tiene que:

$$E_1 \cdot \ldots \cdot E_K = E_1(E_2(\ldots(E_K)\ldots))$$

El campo $E_1 \cdot \ldots \cdot E_K \cdot E_{K+1}$, es el mínimo subcampo de E m $E_i \subseteq E$, $\forall i \in [\![1, K+1]\!]$. Ahora, el campo

$$E_1(E_2(\cdots(E_K(E_{K+1}))\ldots))$$

es el mínimo subcampo que contiene a E_1 y a $E_2(\cdots(E_K(E_{K+1}))\ldots) = E_2 \cdot \ldots \cdot E_K \cdot E_{K+1}$, i.e es el mínimo subcampo que contiene a E_1 y E_i, $\forall i \in [\![2, K+1]\!]$, i.e $E_i \subseteq E_1(\ldots(E_{K+1})\ldots)$, $\forall i \in [\![1, K+1]\!]$. Por tanto:

$$E_1 \cdot \ldots \cdot E_K \cdot E_{K+1} = E_1(E_2(\ldots(E_K(E_{K+1}))\ldots))$$

lo cual prueba el caso $n=K+1$. Por ind. se cumple $\forall n \in \mathbb{N}$.

$\square$

5. Sean E/F una extensión de campos y $\alpha, \beta \in E$. Pruebe que si β es algebraico sobre $F(\alpha)$, donde β es transcendente sobre F, entonces α es algebraico sobre $F(\beta)$.

Dem.

Como β es algebraico sobre $F(\alpha)$, existe $f(x) \in F(\alpha)[x]$ m $f(\beta) = 0$. Es decir:

$$f(x) = \frac{f_0(\alpha)}{g_0(\alpha)} + \frac{f_1(\alpha)}{g_1(\alpha)} x + \ldots + \frac{f_n(\alpha)}{g_n(\alpha)} x^n, \quad f_n(x) \neq 0.$$

donde $f_i(x), g_i(x) \in F[x]$, $g_i(\alpha) \neq 0$, $\forall i \in [\![0, n]\!]$, y:

$$f_i(x) = a_{i0} + a_{i1}x + \ldots + a_{im}x^m, \quad \&$$

$$g_i(x) = b_{i0} + b_{i1}x + \ldots + b_{im}x^m$$

Se tiene ent. que:

$$\begin{aligned}
0 &= f(\beta) \\
&= \sum_{i=0}^{n} \frac{f_i(\alpha)}{g_i(\alpha)} \beta^i \\
&= \sum_{i=0}^{n} \frac{f_i(\alpha) \cdot h_i(\alpha)}{\prod_{j=1}^{m} g_j(\alpha)} \beta^i, \quad \text{donde } h_i(x) = \prod_{\substack{k=0 \\ k \neq i}}^{m} g_k(x) \in F[x] \\
&= \frac{1}{G(\alpha)} \cdot \sum_{i=0}^{n} f_i(\alpha) h_i(\alpha) \beta^i, \quad \text{donde } G(x) = \prod_{k=0}^{m} g_k(x) \in F[x],\ G(\alpha) \neq 0.
\end{aligned}$$

$$= \frac{1}{G(\alpha)} \cdot \sum_{i=0}^{n} F_i(\alpha)\beta^i, \text{ donde } F_i(x) = f_i(x)h_i(x) \in F[x], \text{ y}$$

$$F_i(x) = C_{i0} + C_{i1}x + \dots + C_{ip}x^p, \forall i \in [\![0, n]\!], \; p = \max\{\text{grad}(F_i(x)) \mid F_i(x) \neq 0\}$$

$$\Rightarrow 0 = \frac{1}{G(\alpha)} \cdot \sum_{i=0}^{n} \sum_{j=0}^{p} C_{ij}\alpha^j \beta^i$$

$$\Rightarrow 0 = \sum_{j=0}^{p} \left(\sum_{i=0}^{n} C_{ij}\beta^i \right) \alpha^j$$

Con $\sum_{i=0}^{n} C_{ij_0}\beta^i \neq 0$ para algún $j_0 \in [\![0, p]\!]$, pues $C_{nj_0} \neq 0$ para algún $j_0 \in [\![0, p]\!]$, ya que

$$f_n(x)h_n(x) = F_n(x)$$

$$= C_{n0} + C_{n1}x + \dots + C_{np}x^p$$

donde $f_n(x), h_n(x) \neq 0$, y al ser no cero los polinomios y β trascendente sobre F, no puede suceder que $\sum_{i=0}^{n} C_{ij_0}\beta^i = 0$ para el j_0 ant. Luego, sean

$$l_j(x) = \sum_{i=0}^{n} C_{ij}x^i \in F[x]$$

ent.

$$0 = \sum_{j=0}^{p} l_j(\beta)\alpha^j$$

$$= \frac{l_0(\beta)}{1} + \frac{l_1(\beta)}{1}\alpha + \dots + \frac{l_p(\beta)}{1}\alpha^p$$

donde $\frac{l_j(\beta)}{1} \in F(\beta)$, y como $\frac{l_{j_0}(\beta)}{1} \neq 0$, el polinomio

$$\sum_{j=0}^{p} \frac{l_j(\beta)}{1} x^j \in F(\beta)[x]$$

y es no cero, con α raíz del mismo. Así, α es algebraico sobre $F(\beta)$. $\square$

6. Sean E/F una extensión de campos y $\alpha \in E$ algebraico de grado impar sobre F. Demuestre que α^2 es de grado impar sobre F, y que $F(\alpha) = F(\alpha^2)$.

Dem.

Como $\alpha \in E$ es algebraico de grado impar sobre F, $grad(irr(\alpha, F)) = 2n-1$, donde $n \in \mathbb{N}$. Tenemos 2 casos:

i) $n=1 \Rightarrow grad(irr(\alpha,F)) = 1$, i.e $irr(\alpha, F) = x - c$, donde $c \in F$. Pero α es raiz de este polinomio, i.e

$$\alpha - c = 0 \Rightarrow c = \alpha$$

luego $\alpha \in F$. Asi $\alpha^2 \in F$ y se sigue que $F(\alpha) = F = F(\alpha^2)$, donde el grado de α^2 es 1 (impar) pues α^2 es raiz de $x - \alpha^2 \in F[x]$.

ii) $n > 1 \Rightarrow grad(irr(\alpha, F)) = 2m+1, m \in \mathbb{N}$. Como $\alpha^2 \in F(\alpha)$ y $F(\alpha)$ es campo, ent. $F(\alpha^2) \subseteq F(\alpha)$. Por ende $F \subseteq F(\alpha^2) \subseteq F(\alpha)$ es una torre de campos, donde al ser multiplicativo el grado de la extensión, se tiene que

$$[F(\alpha):F] = [F(\alpha):F(\alpha^2)] \cdot [F(\alpha^2):F]$$

$$\Rightarrow 2m+1 = [F(\alpha):F(\alpha^2)] \cdot [F(\alpha^2):F] < \infty$$

la única forma en que el producto de éstos dos números naturales sea impar, es que ambos lo sean. En particular:

$$[F(\alpha^2):F] = 2K-1, \ K \in \mathbb{N}$$

Por tanto, α^2 es de grado impar sobre F. Para la otra parte, notemos que $F(\alpha^2) \subseteq F(\alpha)$. Probaremos que $\alpha \in F(\alpha^2)$. Sea $g(x) = irr(\alpha^2, F, x) \in F[x]$, i.e:

$$g(x) = b_0 + b_1 x + \ldots + b_l x^l$$

donde $l = 2K-1$. Ent.

7. Sea E/F una extensión de campos, y suponga que $f(X) = X^n - a \in F[X]$ es irreducible, donde $\alpha \in E$ es raíz de $f(X)$. Sea $m \in \mathbb{N}$ tal que m divide a n. Pruebe que el grado de α^m sobre F es n/m. ¿Cuál es el polinomio irreducible de α^m sobre F?

Dem.

Como $m \mid n$, $\exists\, K \in \mathbb{N}$ ⊓ $mK = n$. i.e $n/m = K$. Como α es raiz de $f(x) \in F[x]$, entonces $\alpha \in E$ es algebraico sobre F. Probaremos que $f(x) = irr(\alpha, F, x)$. En efecto,

Como α es raiz de $f(x)$, entonces $\exists\, q(x) \in F[x]$ ⊓

$$f(x) = q(x)\, irr(\alpha, F, x)$$

Pero $f(x)$ es irreducible, ent. $q(x) \in F$ o $irr(\alpha, F, x) \in F$, pero $irr(\alpha, F, x) \notin F$. Por tanto $q(x) \in F$. Como tanto $f(x)$ como $irr(\alpha, F, x)$ son mónicos, ent. $q(x) = 1$.

$$\therefore f(x) = irr(\alpha, F, x)$$

de esta forma, $[F(\alpha) : F] = n$. Como $\alpha^m \in F(\alpha)$, ent. $F(\alpha^m) \subseteq F(\alpha)$. Se tiene la torre de campos $F \subseteq F(\alpha^m) \subseteq F(\alpha)$. Luego

$$[F(\alpha) : F] = [F(\alpha) : F(\alpha^m)] \cdot [F(\alpha^m) : F]$$

$$\Rightarrow \quad n = [F(\alpha) : F(\alpha^m)] \cdot [F(\alpha^m) : F]$$

8. Sea E/F extensión algebraica. Demuestre que cada subanillo de E que contiene a F es un campo. ¿Esto es verdad si la extensión E/F no es algebraica? Pruebe ó de un contraejemplo.

Dem.

Sea $K \subseteq E$ un subanillo de E $\ni$ $F \subseteq K$. Como K es subanillo, $a, b \in K \Rightarrow ab, a-b \in K$, por lo que, para probar que es campo, basta ver que si $a \neq 0$, ent. $a^{-1} \in K$.

Sea $\alpha \in K \setminus \{0\} \subseteq E$. Como E/F es una extensión algebraica, $\exists\ f(x) \in F[x]$ $\ni$ $f(\alpha) = 0$, digamos

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n$$
$$\Rightarrow f(\alpha) = a_0 + a_1\alpha + \ldots + a_n \alpha^n = 0$$

Podemos suponer que $a_0 \neq 0$. Si $a_0 = 0$, sea $i_0 \in [\![1, n]\!]$ el mínimo índice para el cual $a_{i_0} \neq 0$, ent.

$$\begin{aligned} f(\alpha) &= a_{i_0}\alpha^{i_0} + \ldots + a_n \alpha^n \\ &= \alpha^{i_0}(a_{i_0} + \ldots + a_n \alpha^{n-i_0}) \\ &= 0 \end{aligned}$$

como $\alpha \neq 0 \Rightarrow \alpha^{i_0} \neq 0 \Rightarrow a_{i_0} + \ldots + a_n \alpha^{n-i_0} = 0$ donde $a_{i_0} \neq 0$, por lo que basta tomar ese polinomio.

Ent.

$$a_{i_0} = -a_1\alpha - \ldots - a_n \alpha^n$$
$$\Rightarrow 1 = -a_{i_0}^{-1} a_1 \alpha - \ldots - a_{i_0}^{-1} a_n \alpha^n$$
$$\Rightarrow \alpha^{-1} = -a_{i_0}^{-1} a_1 - \ldots - a_{i_0}^{-1} a_n \alpha^{n-1}$$

donde $a_i \in F \subseteq K$, $\forall\, i \in [\![1, n]\!]$, $a_{i_0}^{-1} \in F \subseteq K$ (pues F es campo) y $\alpha, \alpha^2, \ldots, \alpha^{n-1} \in K$. Luego $\alpha^{-1} \in K$. Por tanto, K es campo.

Considero la extensión $\mathbb{R}/\mathbb{Q}$. $\pi \in \mathbb{R}$ es trascendente sobre $\mathbb{Q}$. El subanillo

$$\mathbb{Q}[\pi] = \{ f(\pi) \mid f \in \mathbb{Q}[x] \}$$

Afirmamos que no es campo. Si $\pi^{-1} \in \mathbb{Q}[\pi]$, ent. $\exists\ f(x) \in \mathbb{Q}[x]$ $\ni$

$$\pi^{-1} = a_0 + a_1\pi + \ldots + a_n \pi^n$$
$$\Rightarrow 1 = a_0\pi + a_1\pi^2 + \ldots + a_n \pi^{n+1}$$
$$\Rightarrow 0 = -1 + a_0\pi + a_1\pi^2 + \ldots + a_n \pi^{n+1}$$

i.e π es raiz de $g(x) = -1 + a_0 x + \ldots + a_n x^{n+1} \in \mathbb{Q}[x] \setminus \{0\}_{\neq c_1}$ pues π es trascendente sobre $\mathbb{Q}$.

luego $\pi^{-1} \notin \mathbb{Q}[\pi] \Rightarrow \mathbb{Q}[\pi]$ no puede ser campo.

$\square$

9. Sean E/F una extensión de campos, y $\alpha, \beta \in E$ algebraicos sobre F de grados n y m respectivamente. Pruebe que $[F(\alpha,\beta) : F] \leq nm$. Si n y m son primos relativos, entonces $[F(\alpha,\beta) : F] = nm$.

Dem.

Considere la torre de campos $F \subseteq F(\alpha) \subseteq F(\alpha,\beta)$. Se tiene que:

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

donde $[F(\alpha):F] = n$. Afirmamos que $[F(\alpha,\beta):F(\alpha)] = [F(\alpha)(\beta):F(\alpha)] \leq m$. En efecto, como $[F(\beta):F] = m$, $\exists$ $f(x) \in F[x]$ polinomio mónico de grado m $\ni$

$$f(\beta) = 0$$

en part. $f(x) \in F(\alpha)[x]$ y β es raíz de $f(x)$, luego $\operatorname{irr}(\beta, F(\alpha), x) \mid f(x) \Rightarrow m \geq \operatorname{grad}(\operatorname{irr}(\beta, F(\alpha), x)) = [F(\alpha,\beta):F(\alpha)]$. Por tanto:

$$[F(\alpha,\beta):F] \leq nm$$

Suponga que n y m son primos rel. Por la part. ant. $[F(\alpha,\beta):F(\alpha)] \leq m$. Sea

$$\begin{aligned} g(x) &= \operatorname{irr}(\beta, F(\alpha), x) \\ &= f_0(\alpha) + f_1(\alpha)x + \ldots + f_m(\alpha)x^m \end{aligned}$$

(pues $F(\alpha) = F[\alpha]$ y $f_i(x) \in F[x]$). Digamos

$$f_i(x) = b_{i0} + b_{i1}x + \ldots + b_{il}x^l$$

$\forall i \in [\![0,m]\!]$, $l \in \mathbb{N}$ $\ni$ $l = \text{máx}\{\operatorname{grad}(f_i(x)) \mid f_i(x) \neq 0\}$. Ent.

$$\begin{aligned} 0 &= g(\beta) \\ &= \sum_{i=0}^{m} f_i(\alpha)\beta^i \\ &= \sum_{i=0}^{m}\left(\sum_{j=0}^{l} b_{ij}\alpha^j\right)\beta^i \end{aligned}$$

10. Sean L, M subcampos intermedios de la extensión E/F. Pruebe lo siguiente:

a) $[LM : F]$ es finito si, y sólo si $[L : F]$ y $[M : F]$ son finitos;
b) $[LM : F]$ finito implica que $[L : F]$ y $[M : F]$ dividen a $[LM : F]$, y que $[LM : F] \leq [L : F][M : F]$;
c) Si $[L : F]$ y $[M : F]$ son finitos y primos relativos, entonces $[LM : F] = [L : F][M : F]$.
d) Si $[L : F]$ y $[M : F]$ son finitos con $[LM : F] = [L : F][M : F]$, entonces $L \cap M = F$.
e) Demuestre que la recíciproca de (d) es cierta si $[L : F] = 2$ o $[M : F] = 2$.
f) Use una raíz real y una raíz cúbica no real de 2 para dar un ejemplo donde $L \cap M = F$, $[L : F] = [M : F] = 3$ pero que $[LM : F] < 9$.

Dem.

$$\begin{tikzcd}[column sep=small] & E \arrow[d, dash] & \\ & LM \arrow[dl, dash] \arrow[dr, dash] & \\ L \arrow[dr, dash] & & M \arrow[dl, dash] \\ & F & \end{tikzcd}$$

De a):

$\Rightarrow$) Suponga que $[LM : F] < \infty$. En particular, al ser multiplicativo el índice, se sigue que:

$$[LM:F] = [LM:M][M:F] < \infty$$
$$= [LM:L][L:F] < \infty$$

i.e. $[L:F], [M:F] < \infty$.

$\Leftarrow$) Suponga que $[L:F], [M:F] < \infty$, ent. L/F y M/F son finitas, luego algebraicas y f.g, en part. L/F lo es, i.e $\exists \{u_1, \dots, u_n\} \subseteq L \ni L = F(u_1, \dots, u_n)$ y M/F es algebraica. Luego:

$$LM = ML$$
$$= MF(u_1, \dots, u_n), \text{ como } F \subseteq M$$
$$= M(u_1, \dots, u_n)$$

i.e LM/M es f.g. Veamos que es algebraica. Basta ver que si $\alpha \in L$, α es algebraico sobre M. En efecto, L/F es algebraica, ent. $\exists f(x) \in F[x] \subseteq M[x] \ni$

$$f(\alpha) = 0$$

luego α es algebraico sobre M. Así LM/M es algebraica y f.g. $\Rightarrow$ LM/M finita y:

$$\Rightarrow [LM:F] = [LM:M] \cdot [M:F] < \infty$$

De b): La primera parte es inmediata de a).

11. Sea $E = F(\alpha)$ de grado cinco sobre F. Pruebe que $E = F(\alpha^3)$.

12. Sean $m, n \in \mathbb{N}$. Sean $p_1, \ldots, p_n, q_1, \ldots, q_m$, $m+n$ números primos distintos. Pruebe que

Dem.

Como $F(\alpha)$ es de grado 5 sobre F, ent. $\exists$ $f(x) = a + bx + cx^2 + dx^3 + ex^4 + fx^5 \in F[x]$ m

$$f(\alpha) = 0$$

Como $\alpha \in E$, ent. $\alpha^3 \in E \Rightarrow F(\alpha^3) \subseteq E$.

12. Sean $m, n \in \mathbb{N}$. Sean $p_1, \ldots, p_n, q_1, \ldots, q_m$, $m+n$ números primos distintos. Pruebe que $\sqrt{q_1 \cdots q_m} \notin \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$ y que $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$.

13. Sea $F(X_1,\ldots,X_n)$ el campo de funciones racionales sobre el campo F en las indeterminadas $X_1,\ldots,X_n$. Pruebe que todo elemento de $F(X_1,\ldots,X_n)\setminus F$ es transcendente sobre F.

Dem.

Recordemos que:

$$F(x_1,\ldots,x_n)=\left\{\frac{f(x_1,\ldots,x_n)}{g(x_1,\ldots,x_n)} \,\middle|\, f(x_1,\ldots,x_n), g(x_1,\ldots,x_n)\in F[x_1,\ldots,x_n] \text{ y } g(x_1,\ldots,x_n)\neq 0\right\}$$

Basta probar el caso en que $n=1$, pues en tal caso todo elemento de $F(x_1,\ldots,x_n)\setminus F(x_1,\ldots,x_{n-1})$ es trascentente sobre $F(x_1,\ldots,x_{n-1})$ y si $E\subseteq K\subseteq H$ es una torre de campos dónde $\alpha\in E$ es trascendente sobre K, también lo es sobre H.

Así, sea $\frac{f(x_1)}{g(x_1)}\in F(x_1)\setminus F$. Suponga que $u=\frac{f(x_1)}{g(x_1)}$ es algebraico sobre F, ent. $\exists$ $h(x)\in F[x]$ irreducible m

$$h(u)=0, \text{ digamos } h(x)=a_0+a_1x+\ldots+a_nx^n \quad (a_n\neq 0)$$

$$\Rightarrow 0=a_0+a_1\frac{f}{g}+\ldots+a_n\frac{f^n}{g^n}$$
$$=a_0+a_1\frac{f(x_1)}{g(x_1)}+\ldots+a_n\frac{f^n(x_1)}{g^n(x_1)}\in F(x_1)$$

Pero, como $0\in F(x_1)$ ent.

$$a_0+a_1\frac{f(x_1)}{g(x_1)}+\ldots+a_n\frac{f^n(x_1)}{g^n(x_1)}=\frac{f_1(x_1)}{g_1(x_1)}$$

dónde $f_1(x_1)=0$. Ent.

$$a_0g^n(x_1)+a_1g^{n-1}(x_1)f(x_1)+\ldots+a_nf^n(x_1)=f_1(x_1)=0 \quad \ldots (1)$$

Se tienen 3 casos:

i) $\text{grad}(f(x_1))>\text{grad}(g(x_1))$, ent. el coeficiente dominante de (1) es $a_nb_m^n$, con $f(x_1)=b_0+\ldots+b_mx^m$, $b_m\neq 0$, luego $a_nb_m^n=0$, pero $a_n\neq 0$ y $b_m^n\neq 0$ $\divideontimes$. Por tanto, u es trascendente sobre F.

ii) $\text{grad}(g(x_1))>\text{grad}(f(x_1))$. Sea $n_0\in\mathbb{N}$ el primer natural m $a_{n_0}\neq 0$. Tenemos que el coef. dominante de (1) es el dominante de $a_{n_0}g^{n-n_0}(x_1)f^{n_0}(x_1)$.

Como $f(x_1)=b_0+\ldots+b_mx^m$ y $g(x_1)=c_0+\ldots+c_rx^r$, ent. el coef. dom. es:

$$a_{n_0}c_r^{n-n_0}b_m^{n_0}=0$$

$\Rightarrow c_r=0$ o $b_m=0$ $\divideontimes$, pues ambos son no cero. Por tanto, u es trascendente sobre F.

iii) $\text{grad}(f(x_1))=\text{grad}(g(x_1))$. El coef. dominante de (1) es: $(r=m)$

$$a_0c_m^n+a_1c_m^{n-1}b_m+\ldots+a_nb_m^n=0$$

$$\Rightarrow a_0 + a_1\left(\frac{b_m}{c_m}\right) + \dots + a_n\left(\frac{b_m}{c_m}\right)^n = 0$$

$\Rightarrow b_m c_m^{-1}$ es raiz de $h(x)$. Luego

$$h(x) = (x - b_m c_m^{-1})\, g(x)$$

dónde $g(x) \in F[x]$ es irreducible ~~c~~, pues $h(x)$ es irreducible. Por tanto, $u = \frac{f(x_1)}{g(x_1)}$ es trascendente sobre F.

$\square$

14. Sea $F(X)$ el campo de funciones racionales en la indeterminada X sobre F. Sea $Y = f(X)/g(X)$ elemento no cero de $F(X)$ con $(f(X), g(X)) = 1$. Se define el **grado** de Y como:

$$\deg(Y) = \max\{\deg(f), \deg(g)\}.$$

Pruebe lo siguiente:

a) $F(X)/F(Y)$ es una extensión finita de grado $\deg(Y)$, siempre que $\deg(Y) \geq 1$;

b) $F(X) = F(Y)$ si, y sólo si

$$Y = \frac{aX + b}{cX + d}$$

con $ad - bc \neq 0$.

Dem.

De a): Suponga que $\deg(Y) \geqslant 1$. Probaremos que $F(X)/F(Y)$ es extensión finita de grado $\deg(Y)$.

Veamos que:

$$F(Y) = \left\{ \frac{h(Y)}{l(Y)} \;\middle|\; h(x), l(x) \in F[x] \text{ y } l(Y) \neq 0 \right\}$$

15. Sean E/F una extensión de campos, X, Y indeterminadas algebraicamente independientes sobre F, es decir, no existe un polinomio no cero $f(X_1, X_2) \in F(X_1, X_2)$ tal que $f(X, Y) = 0$. Encuentre dos elementos $\alpha, \beta \in E$ los cuales son transcendentes sobre F y tales que $F(\alpha, \beta) \not\cong F(X, Y)$.

Dem.

Si E/F es algebraica, tales α y β no existen. Suponga que E/F es truscendente y sea

$$K = \{\alpha \in E \mid \alpha \text{ es algebraico sobre } F\}$$

Se sabe que K es un campo $\ni$ $E \supseteq K \supseteq F$. Como E/F es trascendente, $\exists\, \alpha \in E \ni \alpha$ es trascendente sobre F. Afirmamos que $\alpha^{-1} \in E$ también es truscentente sobre F, pues si fuera algebraico, al ser K campo $\Rightarrow \alpha \in K_{\#c}$.

Así, tenemos que α y α^{-1} son truscententes sobre F y

$$\alpha \neq \alpha^{-1}$$

Considere la extensión $F(\alpha, \alpha^{-1})$. Claro que $F(\alpha) \subseteq F(\alpha, \alpha^{-1})$. Como $\alpha^{-1} \in F(\alpha)$, pues $F(\alpha)$ es campo, se sigue que $F(\alpha) = F(\alpha, \alpha^{-1})$.

Al ser α trascendente sobre F, por una prop. se tiene que $F(\alpha) \cong F(x)$, i.e:

$$F(\alpha, \alpha^{-1}) \cong F(x)$$

Afirmamos que $F(x) \not\cong F$. El resultado es inmediato si F es finito. Suponga que F no es finito y considere $f : F(x) \to F$. En part. $F[x] \hookrightarrow F$. Como $F \hookrightarrow F[x] \Rightarrow$

$$F[x] \cong F$$

$\Rightarrow F[x]$ es un campo$_{\#c}$, pues ningún elemento no cte. es invertible. Luego:

$$F(\alpha, \alpha^{-1}) \cong F(x) \not\cong F(x, y)$$

$$\Rightarrow F(\alpha, \alpha^{-1}) \not\cong F(x, y)$$

$\square$

16. Sea $F(X)$ el campo de funciones racionales sobre el campo F, y sea $u = X^3/(X+1)$. Demuestre que $F(X)$ es extensión simple de $F(u)$. Calcule el grado $[F(X) : F(u)]$ y el polinomio $irr(X, F(u), Y)$.

Dem.

Probaremos que $F(x)/F(u)$ es extensión simple. En efecto, veamos que

$$F(x) = F(u)(v)$$

donde $v = \frac{x+1}{x^2} \in F(x)$. En efecto, notemos que $F(u)(v) = F(u,v)$. En part. ya se tiene que $F(u)(v) \subseteq F(x)$, pues $F, \{u\}, \{v\} \subseteq F(x)$.

Para ver que $F(x) \subseteq F(u,v)$, basta con probar que $x \in F(u,v)$. En efecto, como $u, v \in F(u,v)$

$$\Rightarrow u \cdot v = \frac{x^3}{x+1} \cdot \frac{x+1}{x^2} = \frac{x}{1} = x \in F(u,v)$$

$\therefore F(x)/F(u)$ es extensión simple.

17. Sea $E = K(X)$ el campo de funciones racionales sobre el campo K, y sea F subcampo de E que contiene propiamente a K. Pruebe que X es algebraico sobre F.

Dem.

Al ser la contención propia, $\exists\ f(x)/g(x) \in F$, digamos $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, $a_n \neq 0$. Suponga que x es trascendente sobre F.

Afirmamos que x^k es trascendente sobre F, $\forall\ k \in \mathbb{N}$. Se procederá por inducción. Si x^2 fuera alg. sobre F, $\exists\ f(t) \in F[t]$ m

$$f(x^2) = 0, \text{ digamos } f(t) = a_0 + a_1 t + \ldots + a_n t^n,\ a_n \neq 0.$$

ent. x es raíz de $g(t) = a_0 + a_1 t^2 + \ldots + a_n t^{2n}$, pues:

$$g(x) = f(x^2) = 0$$

Con $g(t) \in F[t]$. Luego x^2 es trascendente. El paso inductivo es análogo. Por tanto, el conjunto:

$$\{ b_1 x + \ldots + b_n x^n \mid b_i \in K,\ i \in [\![1, n]\!];\ n \in \mathbb{N} \}$$

Contiene elementos trascendentes sobre F.

bre

18. En el campo $\mathbb{C}$, demuestre que los siguientes campos no son isomorfos:

a) $\mathbb{Q}(i)$ y $\mathbb{Q}(\sqrt{2})$;
b) $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{5})$;
c) $\mathbb{Q}(\sqrt{3})$ y $\mathbb{Q}(\sqrt[3]{3})$.

Pruebe que en (a) y (b) los campos son isomorfos como espacios vectoriales.

Dem.

De a): Suponga que lo son, ent. $\exists f: \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(i)$ isomorfismo. En part. $\exists a \in \mathbb{Q}(\sqrt{2})$ $\ni$

$$f(a) = i \Rightarrow (f(a))^2 = -1$$
$$\Rightarrow f(a^2) = -f(1)$$
$$\therefore a^2 = -1$$

con $a \in \mathbb{Q}(\sqrt{2})$, i.e $\exists$ $p, q \in \mathbb{Q}$ $\ni$ $a = p + q\sqrt{2}$. así:

$$p^2 + 2\sqrt{2}pq + 2q^2 = -1$$

$\Rightarrow p = 0$ o $q = 0 \Rightarrow q \notin \mathbb{Q}$ o $p \notin \mathbb{Q}$ #c. Luego $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(i)$ no son isomorfos.

De (b):

19. Pruebe que E/F es extensión algebraica si y sólo si para cada campo intermedio K y para cada F-monomorfismo $\sigma : K \longrightarrow K$ se tiene que σ es un F-automorfismo de K.

20. Sean E/F y L/F extensiones de campos con E/F extensión algebraica, y sea $\sigma : E \longrightarrow L$ un F-homomorfismo. Pruebe lo siguiente:

   a) $\sigma(E)/F$ es una extensión algebraica.

   b) $[\sigma(E) : F] = [E : F]$.

Notas.