

## Primer parcial - Soluciones

---

**Ejercicio 1.** Sea  $E/F/K$  una torre de extensiones finitas. Probar que:

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

**Solución 1.** Este es un ejercicio bastante teórico así que un par de observaciones y recordatorios no están de más. Recordemos que un cuerpo  $L$  es algebraicamente cerrado si todo polinomio no constante en  $L[x]$  tiene una raíz en  $L$ . Una clausura algebraica de  $K$  es una extensión algebraica de  $K$  que es algebraicamente cerrada. Gabriel probó en clase que la clausura algebraica de un cuerpo  $K$  es única a menos de isomorfismo, luego se justifica la notación  $\bar{K}$ . Una pequeña observación es que  $\bar{K}$  es clausura algebraica para cualquier extensión algebraica de  $K$ , ya que la clase de extensiones algebraicas es distinguida. En particular,  $\bar{K}$  es una clausura algebraica para cualquier extensión finita  $E/K$  pues una extensión de grado finito sobre  $K$  es algebraica sobre  $K$ . Entonces, si tenemos una torre de extensiones finitas  $E/F/K$ , podemos fijar  $\bar{K}$  que es una clausura algebraica para todos.

Recordemos el importante teorema que probó Gabriel:

**Teorema:** Sea  $E/K$  extensión algebraica,  $L$  algebraicamente cerrado y  $\tau : K \rightarrow L$  morfismo de cuerpos. Entonces existe  $\sigma : E \rightarrow L$  que extiende a  $\tau$ .

**Lema:** Supongamos que tenemos  $E$  extensión de  $F$ ,  $L$  y  $L'$  cuerpos algebraicamente cerrados y tenemos  $\sigma : F \rightarrow L$  y  $\tau : F \rightarrow L'$  morfismos de cuerpos. Entonces los conjuntos

$$S_\sigma = \{f \in \text{Hom}(E, L) : f \text{ morfismo de cuerpos}, f|_F = \sigma\}$$

$$S_\tau = \{f \in \text{Hom}(E, L') : f \text{ morfismo de cuerpos}, f|_F = \tau\}$$

están en biyección.

En particular, resulta que  $\#S_\sigma = \#S_\tau$ . Es decir, la cantidad de extensiones no depende ni del cuerpo algebraicamente cerrado elegido ni del morfismo que estamos extendiendo: solo depende de la extensión  $E/F$ .

**Dem:** Como para cualquier  $\bar{\sigma} \in S_\sigma$  la imagen  $\bar{\sigma}(E)$  está contenida en una clausura algebraica de  $\sigma(F)$ , podemos asumir que  $L$  es una clausura algebraica de  $\sigma(F)$ .

Consideramos a  $\sigma$  como un isomorfismo correstrictiendo  $\sigma : F \rightarrow \sigma(F)$  así que lo podemos invertir y considerar  $\sigma^{-1}$ . Por el teorema enunciado podemos extender el morfismo  $\tau \circ \sigma^{-1} : \sigma(F) \rightarrow L'$  a un isomorfismo  $\lambda : L \rightarrow L'$  (resulta un isomorfismo porque  $L$  es algebraicamente cerrado).

El diagrama sería el siguiente:

$$\begin{array}{ccc}
\sigma(F) & \xrightarrow{\tau \circ \sigma^{-1}} & L' \\
\downarrow \text{inc} & \nearrow \lambda & \\
L & & 
\end{array}$$

Ahora, si  $\bar{\sigma} \in S_\sigma$ , entonces  $\lambda \circ \bar{\sigma} : E \rightarrow L'$  es tal que al restringirlo a  $F$  nos queda  $\tau$  porque  $\lambda \circ \bar{\sigma}|_F = \lambda \circ (\bar{\sigma}|_F) = \lambda \circ \sigma$ , como  $\lambda$  está restringida ahora a  $\sigma(F)$ , por el diagrama resulta que  $\lambda \circ \sigma = \tau \circ \sigma^{-1} \circ \sigma = \tau$ , es decir  $\lambda \circ \bar{\sigma} \in S_\tau$ . Esto de hecho nos da una función de  $S_\sigma$  en  $S_\tau$  definida por  $\bar{\sigma} \mapsto \lambda \circ \bar{\sigma}$ . Esta función es claramente inyectiva, luego  $\#S_\sigma \leq \#S_\tau$ .

Haciendo un argumento simétrico obtenemos la otra desigualdad, lo cual prueba la igualdad.  $\square$

Notemos que, de yapa, esto demuestra la buena definición del grado de separabilidad que definió Gabriel  $[E : K]_s = \# \text{Hom}(E/K, \bar{K}/K)$  (tomando  $L = \bar{K}$  y  $L' = \bar{K}'$  y extendiendo  $\iota : K \rightarrow \bar{K}$  donde  $\iota$  es la inclusión y  $\iota' : K \rightarrow \bar{K}'$  también la inclusión).

Por otro lado, sean  $\{\sigma_i\}_{1 \leq i \leq [F:K]_s}$  todos los morfismos en  $\text{Hom}(F/K, \bar{K}/K)$  que son por definición la extensión de  $\iota$  a un morfismo  $\sigma_i : F/K \rightarrow \bar{K}/K$ . Por el lema, cada  $\sigma_i$  se extiende de  $[E : F]_s$  maneras a un  $\sigma_{i,j} : E/K \rightarrow \bar{K}/K$  ( $1 \leq j \leq [E : F]_s$  sin importar quien era  $\sigma_i$  ni la clausura elegida) por lo tanto obtenemos  $[E : F]_s \cdot [F : K]_s$  morfismos distintos en  $\text{Hom}(E/K, \bar{K}/K)$ . En definitiva, obtenemos que  $[E : K]_s \geq [E : F]_s \cdot [F : K]_s$ .

Por otro lado, sea  $\sigma \in \text{Hom}(E/K, \bar{K}/K)$ . Si lo restringimos a  $F$  tenemos un morfismo  $\sigma|_F : F/K \rightarrow \bar{K}/K$ , que es una extensión de  $\iota : K \rightarrow \bar{K}$  y por lo tanto  $\sigma|_F \in \text{Hom}(F/K, \bar{K}/K)$ . Además,  $\sigma : E/K \rightarrow \bar{K}$  es una extensión de  $\sigma|_F$ , luego cualquier  $\sigma \in \text{Hom}(E/K, \bar{K}/K)$  se obtiene como una doble extensión de  $\iota : K \rightarrow \bar{K}$  que nuevamente por el lema se puede hacer de  $[E : F]_s [F : K]_s$  maneras y la igualdad se sigue.  $\square$

**Ejercicio 2.** Sea  $K$  un cuerpo de característica positiva  $p$ , y sea  $f = X^p - X - a \in K[X]$ .

1. Probar que si  $f$  tiene una raíz en  $K$ , entonces tiene  $p$  raíces en  $K$
2. Probar que si  $f$  no tiene raíces en  $K$ , entonces es irreducible. En este caso, probar que el cuerpo de descomposición de  $f$  es una extensión galoisiana de  $K$ , y calcular su grupo de Galois.

**Solución 2.** 1. Supongamos que  $\alpha \in K$  es raíz de  $f$ . Digo que de hecho podemos conocer todas sus raíces, y estas son  $\{\alpha, \alpha + 1, \dots, \alpha + (p-1)\}$  donde  $1, 2, \dots, (p-1)$  son, si pedimos toda la rigurosidad del mundo, los elementos del subcuerpo de  $K$  que se identifica con  $\mathbb{F}_p$ . Notemos que son todas distintas y que están en  $K$ , así que si probamos que son raíces habremos probado el ítem.

En efecto sea  $b \in \{1, \dots, p-1\}$ , entonces:

$$(\alpha + b)^p - (\alpha + b) + a \stackrel{Frob}{=} \underbrace{\alpha^p - \alpha + a}_{0} + b^p - b \stackrel{P.T.F.}{=} b - b = 0$$

Así que en efecto si  $f$  tiene una raíz en  $K$ , entonces tiene a sus  $p$  raíces en  $K$ .

- Supongamos que tenemos una factorización en irreducibles de  $f$  en  $K[x]$  de la forma  $\prod_{i=1}^k f_i(x)$  donde cada  $f_i$  es un polinomio irreducible de grado  $d_i$ . Sea  $\beta$  una raíz de  $f_i$  que, obviamente, es también raíz de  $f$ , y por la misma cuenta que hicimos en el ítem anterior es de la forma  $\beta = \alpha + b$  con  $b \in \mathbb{F}_p$  donde  $\alpha$  alguna raíz en una clausura algebraica de  $K$  (notar que la cuenta de la caracterización de todas las raíces no dependía en ningún momento de que  $\alpha \in K$ ).

Como  $K[\alpha + b] = K[\alpha]$ , tenemos que  $[K[\alpha + b] : K] = d_i = [K[\alpha] : K]$  pero entonces  $d_i = d_j$  para todos  $1 \leq j, i \leq k$ .

Tomando grado, tenemos que  $p = k \cdot d_1$  lo cual es absurdo a menos que  $f$  se factorice en factores lineales en  $K[x]$  (este es el caso  $d_1 = 1$  y  $k = p$ ) o  $f$  sea irreducible en  $K[x]$  (este es el caso donde  $d_1 = p$  y  $k = 1$ ). Concluimos que si  $f$  no tiene una raíz en  $K$ , entonces es irreducible.

Sea  $E$  el cuerpo de descomposición de  $f$ . Ya probamos que es  $K[\alpha]$ , donde  $\alpha$  es una raíz en alguna clausura algebraica. Esta extensión es claramente Galois pues es un cuerpo de descomposición de un polinomio separable. Luego  $|Gal(K[\alpha]/K)| = [K[\alpha] : K] = p$ , que es isomorfo a  $C_p$ .

Como la extensión es simple, si tenemos un automorfismo, este quedará determinado por a donde mandemos  $\alpha$ . Como  $\alpha$  solo puede ir a raíces de su minimal sobre  $K$ , solo podemos obtener a lo sumo  $p$  automorfismos y como  $|Gal(K[\alpha]/K)| = p$ , todos ellos deben definir automorfismos. Es decir,  $Gal(K[\alpha]/K)$  son los  $p$  automorfismos definidos por  $\sigma_b(\alpha) = \alpha + b$  con  $b \in \mathbb{F}_p$ , y está generado por  $\sigma_1$ .

□

**Ejercicio 3.** Sea  $P \in K[X]$  irreducible. Sea  $E/K$  una extensión normal, y supongamos que  $P = \prod_{i=1}^n Q_i^{e_i}$  una factorización de  $P$  como producto de polinomios irreducibles en  $E[x]$ .

- Probar que para todos  $1 \leq i, j \leq n$  se tiene que  $\deg Q_i \deg Q_j$  y  $e_i = e_j$
- Mostrar que esto es falso si la extensión no es normal.

**Solución 3.**

- Sea  $L$  el cuerpo de descomposición de  $f$  sobre  $K$ , que obviamente es normal sobre  $K$ . Usaremos la transitividad de  $\text{Aut}(L/K)$  sobre las raíces de  $f \in K[x]$ , para demostrar que  $\text{Aut}(L/K)$  actúa transitivamente sobre el conjunto de los  $Q_i$ .

Podemos suponer, sin pérdida de generalidad, que todos los polinomios involucrados son mónicos.

Consideramos  $Q_r$  y  $Q_s$ . Existen  $\alpha$  y  $\beta$  en  $L$  raíces de  $Q_r$  y  $Q_s$  respectivamente.

Probamos en una clase que existe un automorfismo  $\sigma : L/K \rightarrow L/K$  que manda  $\alpha \mapsto \beta$  (usamos que existe un isomorfismo  $\hat{\sigma} : K[\alpha]/K \rightarrow K[\beta]/K$  que manda  $\alpha \mapsto \beta$  y el ejercicio 10 de la práctica 2)

Probamos también en el ejercicio 14 de la práctica 2 que  $E \cap L$  es normal sobre  $K$ . Llamemos  $F := E \cap L$ .

Tenemos la torre  $L/F/K$ . Como los coeficientes de  $Q_r$  están en  $E$  y en  $L$  (están en  $L$  porque los coeficientes de un polinomio siempre se pueden pensar como productos y sumas de sus raíces) y como por normalidad  $\sigma(F) \subseteq F$ , resulta que  $Q_r^\sigma \in E[x]$  y tiene como raíz a  $\beta$ . Luego  $Q_s \mid Q_r^\sigma$ . Siendo  $Q_r^\sigma$  irreducible, tenemos que  $Q_s = Q_r^\sigma$ . Hecho esto, digo que:

- (a) En particular, los grados de  $Q_r$  y  $Q_s$  deben ser iguales.
  - (b) Tenemos que  $f^\sigma = f$ , es decir  $\prod_{i=1}^n Q_i^{e_i} = \prod_{i=1}^n (Q_i^\sigma)^{e_i}$ . Por factorización única en  $E[x]$ , debe ser  $e_r = e_s$ , ya que el exponente de  $Q_s$  en el miembro derecho de esta igualdad es  $e_r$ .
2. Usamos nuestro ejemplo preferido, el polinomio  $x^3 - 2 \in \mathbb{Q}[x]$ . Es irreducible en  $\mathbb{Q}[x]$  pues no tiene raíces racionales y en  $\mathbb{Q}[\sqrt[3]{2}]$  se descompone en irreducibles como

$$(x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$$

(el factor  $(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$  contiene a  $\sqrt[3]{2}\xi_3$  y  $\sqrt[3]{2}\xi_3^2$  raíces no reales, así que esto basta para ver que es irreducible en  $\mathbb{Q}[\sqrt[3]{2}] \subseteq \mathbb{R}$  ya que es polinomio de grado 2)

□

**Ejercicio 4.** Sea  $E$  el cuerpo de descomposición del polinomio  $f = (X^4 - 3)(X^3 - 2) \in \mathbb{Q}[X]$ .

- 1. Probar que  $[E : \mathbb{Q}] = 24$
- 2. Hallar todas las subextensiones de  $E$  de grados 3 y 8

**Solución 4.**

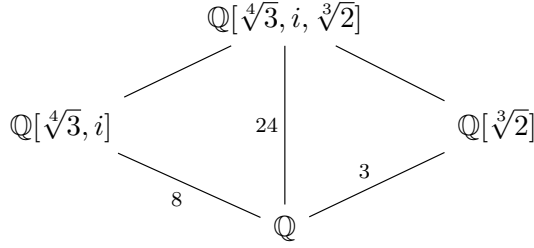
- 1. Las raíces de  $(x^4 - 3)(x^3 - 2)$  son  $\{\sqrt[4]{3}, -\sqrt[4]{3}, i\sqrt[4]{3}, -i\sqrt[4]{3}, \sqrt[3]{2}, \sqrt[3]{2}\xi_3, \sqrt[3]{2}\xi_3^2\}$

Recordemos que  $\xi_3 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$  y  $\xi_3^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$ .

Notemos que  $[\mathbb{Q}[\sqrt[4]{3}, i] : \mathbb{Q}] = [\mathbb{Q}[\sqrt[4]{3}, i] : \mathbb{Q}[\sqrt[4]{3}]] \cdot [\mathbb{Q}[\sqrt[4]{3}] : \mathbb{Q}]$ . Tenemos que  $[\mathbb{Q}[\sqrt[4]{3}] : \mathbb{Q}] = 4$  pues el minimal es  $x^4 - 3$  (Eisenstein), y también  $[\mathbb{Q}[\sqrt[4]{3}, i] : \mathbb{Q}[\sqrt[4]{3}]] = 2$  porque el grado solo puede ser 1 o 2 ( $x^2 + 1$  anula a  $i$ ), pero como  $\mathbb{Q}[\sqrt[4]{3}] \subseteq \mathbb{R}$  resulta que debe ser 2.

Es decir,  $[\mathbb{Q}[\sqrt[4]{3}, i] : \mathbb{Q}] = 8$ .

Entonces podemos hacer un diamante:



El 24 sale claramente de la coprimalidad del 8 con 3.

Faltaría ver que  $\mathbb{Q}[\sqrt[4]{3}, i, \sqrt[3]{2}]$  es el cuerpo de descomposición de este polinomio. Es claro que  $\mathbb{Q}[\sqrt[4]{3}, i, \sqrt[3]{2}] \subseteq E$ , y también es claro que  $E \subseteq \mathbb{Q}[\sqrt[4]{3}, i, \sqrt[3]{2}]$  porque con estos 3 elementos podemos armar cualquier raíz del polinomio (el único truquito aquí es que con  $(\sqrt[4]{3})^2 = \sqrt{3}$  e  $i$  podemos recuperar a  $\xi_3$ ).

2. Veamos cuantos 3-Sylows hay (o sea subgrupos de orden 3). En términos de la notación estándar, tenemos  $n_3 \equiv 1 \pmod{3}$  y  $n_3 | 8$ , o sea que puede haber 1 o 4 subgrupos de orden 3. Digo que hay solo 1. Notemos que la extensión  $\mathbb{Q}[\sqrt[4]{3}, i]$  de grado 8 es normal, luego  $\mathbb{Q}[\sqrt[4]{3}, i] = E^H$  con  $H$  subgrupo normal de orden 3. Pero si un 3-Sylow es normal por los teoremas de Sylow concluimos que solo puede haber uno solo, ya que si agarramos otro 3-Sylow  $J$ , tenemos que  $J = gHg^{-1} = H$ . Concluimos que esta es la única extensión de grado 8.

Veamos cuantos 2-Sylows hay (o sea subgrupos de orden 8). Tenemos que  $n_2 | 3$ , por lo que puede haber 1 o 3 grupos de orden 8. Por la correspondencia de Galois, estos se corresponden con subextensiones de grado 3 sobre  $\mathbb{Q}$ . Notemos que tenemos a  $\mathbb{Q}[\sqrt[3]{2}]$  que es de grado 3 sobre  $\mathbb{Q}$ , también  $\mathbb{Q}[\sqrt[3]{2}\xi_3]$  es de grado 3 sobre  $\mathbb{Q}$ , y no hay dudas de que estas dos subextensiones son distintas (una está contenida en los reales y la otra no). Nos falta una tercera, que digo que es  $\mathbb{Q}[\sqrt[3]{4}\xi_3]$ . Notemos que el minimal de su generador es  $x^3 - 4$  (Eisenstein), luego también es de grado 3. Por el mismo argumento de antes, no hay dudas de que  $\mathbb{Q}[\sqrt[3]{4}\xi_3]$  y  $\mathbb{Q}[\sqrt[3]{2}]$  son distintas. Solo falta ver que  $\mathbb{Q}[\sqrt[3]{4}\xi_3]$  y  $\mathbb{Q}[\sqrt[3]{2}\xi_3]$  no son la misma extensión. Si fueran la misma, entonces  $[\mathbb{Q}[\sqrt[3]{4}\xi_3, \sqrt[3]{2}\xi_3] : \mathbb{Q}] = 3$ , pero notemos que  $(\sqrt[3]{2}\xi_3)^2 = \sqrt[3]{4}\xi_3^2$ , luego en  $\mathbb{Q}[\sqrt[3]{4}\xi_3, \sqrt[3]{2}\xi_3]$  podemos dividir por  $\sqrt[3]{4}\xi_3$  para obtener que  $\xi_3 \in \mathbb{Q}[\sqrt[3]{4}\xi_3, \sqrt[3]{2}\xi_3]$ . Esto automáticamente nos dice que  $[\mathbb{Q}[\sqrt[3]{4}\xi_3, \sqrt[3]{2}\xi_3] : \mathbb{Q}] = 6 \neq 3$  y terminamos.

**Nota:** Quizás es más natural elegir  $\mathbb{Q}[\sqrt[3]{2}\xi_3^2]$  como la otra extensión de grado 3. Notemos que es igual a  $\mathbb{Q}[\sqrt[3]{4}\xi_3]$  (la que yo usé) ya que  $(\sqrt[3]{4}\xi_3)^2 = \sqrt[3]{2}\xi_3^2$  y  $(\sqrt[3]{2}\xi_3^2)^2 = \sqrt[3]{4}\xi_3$ , así que *don't panic* si dijeron que  $\mathbb{Q}[\sqrt[3]{2}]$ ,  $\mathbb{Q}[\sqrt[3]{2}\xi_3]$  y  $\mathbb{Q}[\sqrt[3]{2}\xi_3^2]$  son las 3 subextensiones de grado 3.

□

**Ejercicio 5.** Sea  $K$  un cuerpo finito de  $q$  elementos y sea  $X$  trascendente sobre  $K$ . Sea  $G$  el subgrupo de  $\text{Aut}(K(X)/K)$  generado por los automorfismos  $f_a, g_b$  dados por

$$\begin{aligned} f_a(X) &= aX, & a &\in K^\times; \\ g_b(X) &= X + b, & b &\in K; \end{aligned}$$

Probar que  $K(X)^G = K(Y)$ , con

$$Y = \frac{X^{q^2} - X}{X^q - X}$$

**Solución 5.** Notemos que por ejercicio 16 b) de la práctica 4 los automorfismos de  $K(x)/K$  quedan bien definidos por definir la acción en la indeterminada  $x$  y mandarla a un cociente de polinomios en  $K[x]$  de grado 1. Así, el automorfismo queda completamente y unívocamente determinado en cualquier elemento de  $K(x)$ . Los elementos del enunciado cumplen esto ( $a \in K^\times$ !), así que nos quedamos tranquilos de que definen automorfismos de  $K(x)$ .

Veamos que  $Y$  queda fijo por cada  $f_a$  y cada  $g_b$ . En efecto, usando que Frobenius es un automorfismo de toda extensión de  $K$ ,

$$\begin{aligned} g_b(Y) &= \frac{g_b(x)^{q^2} - g_b(x)}{g_b(x)^q - g_b(x)} = \frac{(x+b)^{q^2} - (x+b)}{(x+b)^q - (x+b)} = \frac{x^{q^2} + b - x - b}{x^q + b - x - b} = Y, \\ f_a(Y) &= \frac{f_a(x)^{q^2} - f_a(x)}{f_a(x)^q - f_a(x)} = \frac{(ax)^{q^2} - (ax)}{(ax)^q - (ax)} = \frac{ax^{q^2} - ax}{ax^q - ax} = Y. \end{aligned}$$

De esto se sigue que  $Y$  queda fijo por el subgrupo  $G$ , por lo que  $K(Y) \subseteq K(x)^G$ . Por el teorema de Artin, la extensión  $K(x)/K(x)^G$  es Galois con  $[K(x) : K(x)^G] = |G|$ . Luego, para concluir la igualdad basta con probar que  $|G| = [K(x) : K(y)]$ .

Para calcular  $[K(x) : K(Y)]$  vamos a “coprimalizar” la función racional  $Y$ , es decir escribir  $Y = f/g$  con  $f, g \in K[x]$  coprimos. Notemos que de hecho todas las raíces de  $x^q - x$  son raíces de  $x^{q^2} - x$  ya que si  $\alpha$  es raíz de  $x^q - x$ , entonces  $\alpha^{q^2} = (\alpha^q)^q = (\alpha)^q = \alpha$ . Además la derivada formal de  $x^q - x$  es  $-1$ , de modo que es un polinomio separable y de esta forma  $x^q - x$  divide a  $x^{q^2} - x$ . Luego  $Y$  es, más que una función racional, un polinomio un de grado  $q^2 - q$ . De esta forma, por ejercicio 16 a) P4 (o 22 P1) tenemos que  $[K(x) : K(y)] = q^2 - q$ .

Para calcular el orden del grupo  $G$ , consideramos los subgrupos  $\langle f_a \rangle_{a \in K^\times}$  y  $\langle g_b \rangle_{b \in K}$ , que tienen órdenes  $q - 1$  y  $q$  respectivamente. Notemos que  $\langle g_b \rangle_{b \in K} \trianglelefteq G$ , ya que que  $f_a \circ g_b \circ f_a^{-1} = g_{ab}$ . Esto muestra que  $G$  tiene a lo sumo  $q^2 - q$  elementos (lo cual alcanza para nuestros propósitos). Pero, más aún, como estos subgrupos se intersecan trivialmente,  $G$  tiene exactamente  $q^2 - q$  elementos.

□