Tarea 13

1. Sea $R := \mathbb{Q}[x_1, ..., x_n]$ el anillo polinomial sobre $\mathbb{Q}$ en las variables x_i y sea L su cuerpo cociente. Los *polinomios simétricos elementales son los elementos* $s_1, ..., s_n \in R$ definidos por:

$$\begin{aligned} s_1 &:= x_1 + ... + x_n, \\ s_2 &:= \sum_{1\le i<j\le n} x_i x_j, \\ &\vdots \\ s_r &:= \sum_{1\le i_1<i_2<...<i_r\le n} x_{i_1}x_{i_2}...x_{i_r} \\ &\vdots \\ s_n &:= x_1 x_2 ... x_n. \end{aligned}$$

- Sea $p(x) \in R[x]$ definido por $p(x) = (x - x_1)(x - x_2)...(x - x_n)$. Muestre que

$$p(x) = x^n - s_1 x^{n-1} + ... + (-1)^r s_r x^{n-r} + ... + (-1)^n s_n.$$

Proof. Podemos probar esto por inducción sobre el grado del polinomio. Primero, para el caso base observese que si $n = 1$ entonces $p(x) = (x - x_1)$ y $s_1 = x_1$ por lo que $f(x) = x - s_1$.
Ahora para el paso inductivo suponga que el enunciado vale para n y queremos demostrar que vale para $n+1$. Entonces tome $f(x)$ un polinomio de grado $n+1$. Por nuestra hipotesis de inducción este polinomio es igual a

$$\begin{aligned} f(x) &= (x^n - s_1 x^{n-1} + ... + (-1)^r s_r x^{n-r} + ... + (-1)^n s_n)(x - x_{n+1}) \\ &= x^{n+1} - s_1 x^n - x_{n+1} x^n + \cdots + (-1)^r s_r x^{n-r+1} - (-1)^{r-1} s_{r-1} x^{n-r+1} x_{n+1} + \cdots + (-1)^{n+1} s_n x_{n+1} \end{aligned}$$

Definimos por s_i los polinomios simétricos elementales de $\mathbb{Q}[x_1, \cdots, x_n]$ y por s'_i los polinomios simétricos elementales de $\mathbb{Q}[x_1, \cdots, x_n, x_{n+1}]$ y además agregamos la convención de que $s_0 = 1$. Entonces tenemos que el $n-1$-ésimo termino x^{n+1} y el término constante $s'_{n+1} = s_n x_{n+1}$ coinciden con la expresión.
Finalmente necesitamos ver que $(-1)^r s_r x^{n-r+1} - (-1)^{r-1} s_{r-1} x^{n-r+1} x_{n+1} = (-1)^r s'_r x^{n-r+1}$. Es decir, que $(s_r + s_{r-1} x_{n+1}) = s'_r$.
Entonces vemos que los términos que deben aparecer en s'_r son por un lado los elementos que aparecian en s_r y por otro lado los elementos que aparecen en s_{r-1} multiplicados por x_{n+1}. Por esta razón, $s_r + s_{r-1} x_{n+1} = s'_r$ y con esto concluimos la demostración.

□

- Sea $S \subseteq R$ el subanillo generado por los polinomios elementales y $\mathbb{Q}$ i.e., $S := \mathbb{Q}[s_1, ..., s_n]$ y sea K su cuerpo cociente. Muestre que L/K es una extensión de Galois y que

$$[L : K] \le n!$$

Proof. La extensión es separable porque estamos sobre un cuerpo de característica 0. Vamos a probar que esta extensión corresponde al cuerpo de partición del polinomio $f(x) = (x - x_1))(x - x_2) \cdots (x - x_n)$, por lo que la extensión también seria normal y por lo tanto de Galoiss. Por el punto anterior tenemos que este polinomio tiene coeficientes en K. Además cada una de las raices pertenecen a L pues las raices x_1 son polinomios que pertenecen a $\mathbb{Q}[x_1, \cdots x_n]$, pero por definición, este sería el mínimo anillo que contiene a estas raices y L sería el mínimo campo que las contiene, es decir que L sería el cuerpo de descomposición. Finalmente, por lo discutido en clase el orden de un cuerpo de descomposición de un polinomio de grado n es a lo sumo $n!$. □

- Muestre que el grupo simétrico S_n actua de manera natural sobre R, donde la acción respeta las operaciones de anillo, y que esta acción se extiende a L. Más aun muestre $K \subseteq \mathrm{Stab}_{S_n}(L)$.

Proof. La acción de grupo natural es tomar $\phi : S_n \times R \to R$ como $\sigma p(x_1, \cdots, x_n) = p(\sigma(x_1), \cdots, \sigma(x_n))$. Esta acción preserva la suma pues
$\sigma(p(x_1, \cdots, x_n) + q(x_1, \cdots, x_n)) = p(\sigma(x_1), \cdots, \sigma(x_n)) + q(\sigma(x_1), \cdots, \sigma(x_n)) = \sigma p(x_1, \cdots, x_n) + \sigma q(x_1, \cdots, x_n)$.
Además preserva la multiplicación pues
$\sigma(p(x_1, \cdots, x_n)q(x_1, \cdots, x_n)) = p(\sigma(x_1), \cdots, \sigma(x_n))q(\sigma(x_1), \cdots, \sigma(x_n)) = \sigma p(x_1, \cdots, x_n)\sigma q(x_1, \cdots, x_n)$.
Entonces podemos extender este homomorfismo a L tomando $\tilde{\phi} : S_n \times L \to L$, como

$$\sigma \frac{p(x_1, \cdots, x_n)}{q(x_1, \cdots, x_n)} = \frac{p(\sigma(x_1), \cdots, \sigma(x_n))}{q(\sigma(x_1), \cdots, \sigma(x_n))}$$

.

Claramente tenemos que esta es una extensión de la acción anterior y además de la misma manera que en el caso anterior podemos demostrar que la acción preserva la multiplicación y la suma. Por otro lado, tenemos que $K \subseteq \mathrm{Stab}_{S_n}(L)$. Esto es así porque los polinomios símetricos que generan a K tienen la propiedad de ser invariantes bajo cualquier permutación, es decir, $\sigma(s_i) = s_i$ para cualquier $0 < i \leq n$ y porque la acción preserva la suma y la multiplicación. □

- Deduzca de los dos incisos anteriores que existe un isomorfismo $S_n \cong \mathrm{Gal}(L/K)$. (La extensión L/K se conoce como *extensión universal* de grado n)

Proof. La acción anterior nos permite definir un homomorfismo inyectivo $S_n \hookrightarrow \mathrm{Gal}$. Tome $\Psi : \sigma \mapsto \phi_\sigma : r \mapsto \sigma r$, para $r \in L$. Cada ϕ_σ es un automorfismo porque la acción preserva la suma y la multiplicación. Además cada σ da un automorfismo diferente. Para probar esto basta considerar el polinomio $x_1 + x_2^2 + \cdots + x_r^r + \cdots + x_n^n$ y darse cuenta que cualesquiera dos permutaciones diferentes dan un polinomio diferente. Pero por el criterio de casillas tenemos que Ψ debe ser sobreyectiva porque $|S_n| = n!$ y $|\mathrm{Gal}(L/K)| \leq n!$ Por lo tanto $S_n \cong \mathrm{Gal}(L/K)$. □

- Sea G un grupo finito. Muestre que existen cuerpos F/E, con F/E de Galois, tal que $\mathrm{Gal}(F/E) \cong G$.

Proof. La teoría de representación de los grupos simétricos nos dice que si G es un grupo de orden n entonces existe un subgrupo H en S_n isomorfo a G. Por lo tanto, si tomamos $R = \mathbb{Q}[x_1, \cdots, x_n]$ y L su campo de fracción y luego tomamos $S = \mathbb{Q}[s_1, \cdots, s_n]$ y K su campo de fracciones, entonces tendriamos que $\mathrm{Gal}(L/K) \cong S_n$ por el punto anterior y luego por el teorema fundamental de la teoría de Galois tendriamos que L^H la subextensión de L^H fijada por el grupo H es tal que $\mathrm{Gal}(L/L^H) \cong H \cong G$. □

- Sea $q(x_1, ..., x_n) \in \mathbb{Q}(x_1, ..., x_n)$ una función racional en la variables x_i. Muestre que si $q(x_1, ..., x_n)$ es invariante bajo cualquier permutación de las variables x_i entonces q se puede escribir como una función racional en las variables $s_1, ..., s_n$ i.e., $q \in \mathbb{Q}(s_1, ..., s_n)$. (De hecho el *teorema fundamental de las funciones simétricas* dice que el analogo para polinomios también es cierto, en otras palabras $\mathrm{Stab}_{S_n}(\mathbb{Q}[x_1, ..., x_n]) = \mathbb{Q}[s_1, ..., s_n]$).

Proof. Por lo demostrado anteriormente el hecho que q sea invariante bajo cualquier permutación significa que $q \in L^{S_n}$ y esto es precisamente igual a K. Por lo tanto q debe ser igual a alguna función racional en $K = \mathbb{Q}(x_1, \cdots, x_n)$. □

- Sea $p(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$. Encuentre $h(s_1, s_2, s_3)$ tal que $p(x_1, x_2, x_3) = h(s_1, s_2, s_3)$.

Proof. Tome $s_1^2 = (x_1 + x_2 + x_3)^2 = x_1^2 + 2x_1(x_2 + x_3) + x_2^2 + 2x_2x_3 + x_3^2 = x_1^2 + x_2^2 + x_3^2 + 2(x_1x_2 + x_1x_3 + x_2x_3) = x_1^2 + x_2^2 + x_3^2 + 2s_2$. Entonces vemos que $x_1^2 + x_2^2 + x_3^2 = s_1^2 - 2s_2$. □

2. Sea L/F una extensión de Galois y sean K_1/F, K_2/F sub-extensiones de Galois de L/F.

- Muestre que K_1K_2/F y $(K_1 \cap K_2)/F$ son extensiones de Galois.

  Proof. Tanto K_1K_2/F como $(K_1 \cap K_2)/F$ son extensiones separables pues ambas son subextensiones de la extensión de Galois L/F que es separable. Entonces cualquier polinomio minimal en K_1K_2/F o en $(K_1 \cap K_2)/F$ es un polinomio minimal en L/F y como aquí es separable se tiene que en los dos primeros también lo es.
  Ahora para probar que K_1K_2/F es normal tenemos que como K_1/F es el cuerpo de dscomposición de una familia A de polinomios y K_2/F es el cuerpo de descomposición de una familia B de polinomios, entonces K_1K_2/F es el cuerpo de descomposición de la familia $A \cup B$, pues contiene todas las raíces de todos los polinomios en $A \cup B$ y es por definición el mínimo cuerpo que puede contener todas estas raíces. Por otra parte $K_1 \cap K_2$ es normal pues si tomamos cualquier polinomio irreducible con una raiz en $K_1 \cap K_2/F$ entonces por un lado todas sus raíces estan incluidas en K_1/F pero también todas estan en K_2/F. Por lo tanto, todas las raices estan incluidas en $(K_1 \cap K_2)/F$. ☐

- Considere el homomorfismo

$$\begin{array}{rccc} \Psi: & \mathrm{Gal}(L/F) & \to & \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F) \\ & \sigma & \mapsto & \left(\mathrm{res}^L_{K_1}(\sigma), \mathrm{res}^L_{K_2}(\sigma)\right) \end{array}$$

  - Muestre que $\mathrm{Ker}(\Psi) = \mathrm{Gal}(L/K_1K_2)$

    Proof. En la tarea anterior vimos que el kernel de $\mathrm{res}^L_{K_1}(\sigma)$ son aquellos automorfismos para los que K_1 es invariante. En este caso el kernel son los automorfismos que dejan fijo tanto a K_1 como a K_2 por lo tanto deben dejar fijo a K_1K_2 que es generado por estos dos campos y es por esta razón que $Ker(\Psi) = \mathrm{Gal}(L/K_1K_2)$. ☐

  - Muestre que $\mathrm{Im}(\Psi) = \mathrm{Gal}(K_1/F) \times_{\mathrm{Gal}((K_1 \cap K_2)/F)} \mathrm{Gal}(K_2/F)$. (Acá el producto fibrado, ver última pagina, es con respecto a los homomorfimos $\mathrm{res}^{K_1}_{K_1 \cap K_2}$ y $\mathrm{res}^{K_2}_{K_1 \cap K_2}$).

    Proof. Tome $\Psi(\sigma) = (\mathrm{res}^L_{K_1}(\sigma), \mathrm{res}^L_{K_2}(\sigma))$. Entonces aplicando los morfismos asociados al grupo fibrado tenemos que $\mathrm{res}^{K_1}_{K_1 \cap K_2}(\mathrm{res}^L_{K_1}(\sigma)) = \mathrm{res}^L_{K_1 \cap K_2}(\sigma)$ y $\mathrm{res}^{K_2}_{K_1 \cap K_2}(\mathrm{res}^L_{K_2}(\sigma)) = \mathrm{res}^L_{K_1 \cap K_2}(\sigma)$, como vemos que ambas aplicaciones son iguales concluimos que $\Psi(\sigma)$ pertenece al producto fibrado.
    Ahora para probar que cualquier elemento en el producto fibrado tome dos automorfismos σ_1 y σ de K_1 y K_2 tales que restringidos a $K_1 \cap K_2$ son iguales. Entonces podemos definir un automorfismo en K_1K_2 a partir de estos automorfismos como $\sigma :\mapsto k_1k_2 \to \sigma_1(k_1)\sigma_2 k_2$ y $k_1 + k_2 \mapsto \sigma_1 k_1 + \sigma_1 k_1$. Este automorfismo esta bien definido porque los dos automorfismos coinciden en $K_1 \cap K_2$ y finalmente podemos extender este automorfismo σ a un automorfismo σ' de L. Luego tenemos que la imagen de σ' va a ser igual a (σ_1, σ_2) por lo que el producto fibrado pertenece a la imagen. ☐

- Concluya que $\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times_{\mathrm{Gal}((K_1 \cap K_2)/F)} \mathrm{Gal}(K_2/F)$. Deduzca que en particular si K_1 y K_2 son sub-extensiones tales que $K_1K_2 = L$ y $K_1 \cap K_2 = F$ se tiene que

$$\mathrm{Gal}(L/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F).$$

  Proof. Por el primer teorema del isomorfismo de grupos tenemos que

$$\mathrm{Gal}(L/F)/\mathrm{Gal}(L/K_1K_2) \cong \mathrm{Gal}(K_1/F) \times_{\mathrm{Gal}((K_1 \cap K_2)/F)} \mathrm{Gal}(K_2/F)$$

  .

  Entonces por el teorema fundamental de la tería de Galois tenemos que $\mathrm{Gal}(L/F)/\mathrm{Gal}(L/K_1K_2) \cong \mathrm{Gal}(K_1K_2/F)$, ya que la extensión K_1K_2/F es normal.
  En particular si $K_1K_2 = L$ y $K_1 \cap K_2 = F$ entonces tendriamos que

$$\mathrm{Gal}(L/F) \cong \mathrm{Gal}(K_1/F) \times_{\mathrm{Gal}(F/F)} \mathrm{Gal}(K_2/F)$$

.

Entonces como $\mathrm{Gal}(F/F) = \{e\}$ el producto fibrado es igual al producto directo y concluimos que

$$\mathrm{Gal}(L/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F).$$

$\square$

- Suponga que $[L : F] = [K_1 : F][K_2 : F]$ y que m.c.d$([K_1 : F], [K_2 : F]) = 1$. Muestre que

$$\mathrm{Gal}(L/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F).$$

Proof. En el parcial demostramos que si esto ocurre entonces $L = K_1K_2$. Además tambien podemos concluir que $K_1 \cap K_2 = F$ pues claramente $F \subseteq K_1 \cap K_2$ y además tenemos por el lema de las torres que $[K_1 : F] = [K_1 : K_1 \cap K_2][K_1 \cap K_2 : F]$ y $[K_2 : F] = [K_2 : K_1 \cap K_2][K_1 \cap K_2 : F]$ por lo que $[K_1 \cap K_2 : F]$ divide al máximo común divisor de $[K_1 : F]$ y $[K_2 : F]$, es decir, debe ser igual a 1. Luego, por el punto anterior concluimos que

$$\mathrm{Gal}(L/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F).$$

$\square$

3. Sean m, n enteros positivos tales que m.c.d$(m, n) = 1$.

(a) Muestre que $\mathbb{Q}(\zeta_{mn}) = \mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)$.

Proof. Tenemos que $\mathbb{Q}(\zeta_m)$ y $\mathbb{Q}(\zeta_n)$ son subextensiones de $\mathbb{Q}(\zeta_{mn})$, pues las n-raíces y m-raices de la unidad estan incluidas en las mn-raices de la unidad. Tenemos que $\zeta_m = (\zeta_{mn})^n$ y $\zeta_n = (\zeta_{mn})^m$. Por lo tanto, $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_{mn})$ Pero además por la identidad de Bezout tenemos que existen enteros a, b tales que $1 = am + bn$ luego $(\zeta_n)^a(\zeta_m)^b = (\zeta_{mn})^{ma+bn} = \zeta_{mn}$. Esto nos permite concluir que $\mathbb{Q}(\zeta_{mn}) = \mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)$. $\square$

(b) Deduzca de (a) que $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.

Proof. En el Dummit tenemos la siguiente igualdad que relacione el cuerpo compuesto con la intersección de cuerpos.
Sea K/F una extensión de Galois y F'/F una extensión finita. Entonces

$$[KF' : F] = \frac{[K : F][F' : F]}{[K \cap F' : F]}.$$

En nuestro caso tendriamos que

$$[\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \frac{[\mathbb{Q}(\zeta_m) : \mathbb{Q}][\mathbb{Q}(\zeta_n) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}]}.$$

Entonces por el punto anterior y por nuestro conocimiento sobre las extensiones ciclotomicas concluimos que

$$[\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}] = \frac{\varphi(m)\varphi(n)}{\varphi(mn)} = 1$$

Esto ultimo porque la función φ de Euler es multiplicativa cuando m y n son primos relativos.
Por lo tanto, $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$. $\square$

(c) Sean $p_1, ..., p_k$ primos distintos y sea $N = \prod_i p_i$. Muestre que

$$\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong \mathbb{Z}/(p_1 - 1)\mathbb{Z} \times ... \times \mathbb{Z}/(p_k - 1)\mathbb{Z}.$$

Proof. El literal anterior nos da las hipotesis para poder utilizar el punto anterior. Podemos probar esto por inducción fuerte sobre el número de factores primos de N.

Cuando $N = p$, entonces tenemos que $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{Z}/\varphi(p)\mathbb{Z} = \mathbb{Z}/(p-1)\mathbb{Z}$.

Ahora por inducción tomemos $N = p_1 \cdots p_{k-1}p_k$. Entonces tenemos por el literal y el punto anterior que $\text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong \text{Gal}(\mathbb{Q}(\zeta_{p_1\cdots p_{k-1}})/\mathbb{Q}) \times \text{Gal}(\mathbb{Q}(\zeta_{p_k})/\mathbb{Q})$. Entonces por hipótesis de inducción $\text{Gal}(\mathbb{Q}(\zeta_{p_1} \cdots p_{k-1})/\mathbb{Q}) \cong \mathbb{Z}/(p_1-1)\mathbb{Z} \times \cdots \times \mathbb{Z}/(p_{k-1}-1)\mathbb{Z}$ Luego $\text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong \mathbb{Z}/(p_1-1)\mathbb{Z} \times \cdots \times \mathbb{Z}/(p_{k-1}-1)\mathbb{Z} \times \mathbb{Z}/(p_k-1)\mathbb{Z}$ y esto concluye la demostración. ☐

(d) Sea G un grupo abeliano finito. Muestre que existe $L/\mathbb{Q}$ extensión de Galois tal que $\text{Gal}(L/\mathbb{Q}) \cong G$.

Proof. Por el teorema fundamental de los grupos abelianos finitos tenemos que $G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \mathbb{Z}/n_r\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$ con $n_1|n_2|\cdots|n_k$ y $n_1 \cdots n_k = |G|$. En clase vimos que existen infinitos primos que satisfacen la ecuación $p \equiv 1 \mod n$ para cualquier $n > 1$. Luego, podemos elegir por cada n_i un primo p_i tal que $p_i \equiv 1 \mod n_i$ y tales que los p_i son diferentes entre sí. Esto significa que n_i divide a $p_i - 1$. Luego si tomamos $\mathbb{Q}(\zeta_{p_i})/\mathbb{Q}$ tenemos que $\text{Gal}(\mathbb{Q}(\zeta_{p_i})/\mathbb{Q}) \cong \mathbb{Z}/(p_i-1)\mathbb{Z}$. Entonces como vimos en la tarea anterior hay una subextensión $K_i/\mathbb{Q}$ de $\mathbb{Q}(\zeta_{p_i})/\mathbb{Q}$ tal que su grupo de Galois es $\mathbb{Z}/n_i\mathbb{Z}$. Por lo demostrado anteriormente podemos tomar $\mathbb{Q}(p_1p_2\cdots p_k)/\mathbb{Q}$ y su grupo de Galois es $\mathbb{Z}/(p_1-1)\mathbb{Z} \times \cdots \times \mathbb{Z}/(p_k-1)\mathbb{Z}$ y por lo tanto $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/(n_k)\mathbb{Z} \cong G$ es normal y tendrá asociada una subextensión $K/\mathbb{Q}$ cuyo grupo de Galois será G. ☐

4. Sea p un primo.

(a) Sea n un entero positivo. Muestre existe $\mathbb{F}_{p^n}/\mathbb{F}_p$ es una extensión de Galois y encuentre un isomorfismo explícito

$$\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}.$$

Proof. En una tarea anterior demostramos que si F'/F es una extensión finita de un campo finito entonces la extensión es separable. Además la extensión es normal por otro punto en una tarea anterior donde demostramos que $/F_{p^n}$ era el cuerpo de descomposición del polinomio $x^{p^n} - x$. Por otra parte, sabemos que $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ por lo que para probar que el grupo de Galois es $\mathbb{Z}/n\mathbb{Z}$ solo nos falta ver que hay un elemento en el grupo de Galois cuyo orden sea n. Ese elemento es el homomorfismo de Frobenius.

Para probar que su orden es n observese que $\mathbb{F}_{p^n}^* \cong \mathbb{Z}/(p^n-1)\mathbb{Z}$ entonces si tomamos cualquier elemento en $a \in \mathbb{F}_{p^n}^*$ tenemos que $a^{p^n-1} = 1$. Luego $a^{p^n} = a$ y como $0^{p^n} = 0$ tenemos que $\text{Frob}_p^n = id$. Pero además el hecho de que en $\mathbb{F}_{p^n}^*$ hay un elemento de orden $p^n - 1$ nos dice que n es el menor número tal que $\text{Frob}_p^n = id$.

Esto porque si $\alpha^k = \alpha$ con $k < m$ y $\alpha^m = 1$ tendriamos que $\alpha^{m-k} = \alpha^{-1} = \alpha^{m-1}$. Por lo que concluiimos que $k = 1$. Así que el orden de Frobenius no puede ser menor a n. ☐

(b) Sean m, n enteros positivos. Muestre que $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ si y sólo si $m \mid n$.

Proof. Tome $\text{Gal}(\mathbb{F}_{p^m}/F) \cong \mathbb{Z}/m\mathbb{Z}$ y $\text{Gal}(\mathbb{F}_{p^n}) \cong \mathbb{Z}/n\mathbb{Z}$. Entonces si $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ entonces tendriamos que $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}/H$ para algun subgrupo H de $\mathbb{Z}/n$ pero si este subgrupo existe tenemos por el teorema de Lagrange que $[\mathbb{Z}/n\mathbb{Z} : H]|H| = m|H| = n$, es decir que $m|n$.

Para la otra dirección observe que si $m|n$ entonces $mk = n$ y por lo tanto, si tomamos el polinomio $x^{p^n-1} - 1 = x^{p^{mk}-1} - 1$. Ahora observese que $p^{mk} - 1$ es divisible por $p^k - 1$. pues $(p^k)^m - 1^m = (p^k-1)((p^k)^{m-1} - (p^k)^{m-2} + \cdots (-1)^{m-1})$. Entonces $x^{p^n-1} - 1 = x^{l(p^k-1)} - 1$ donde $l = ((p^k)^{m-1} - (p^k)^{m-2} + \cdots (-1)^{m-1})$. Pero entonces por la misma razón podemos concluir que $x^{l(p^k-1)} - 1 = (x^{p^k-1})^l - 1^l = (x^{p^k-1} - 1)((x^{p^k-1})^{l-1} - (x^{p^k-1})^{l-2} + \cdots + (-1)^{l-1})$ Por lo tanto, el polinomio $x^{p^n} - x$ es divido por el polinomio $x^{p^m} - x$. Por lo tanto las raices del primero contienen a las raices del segundo, es decir, $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$.

☐

5. Sea $p(x) = x^4 + 2x^3 + 2x^2 + 2 \in \mathbb{Q}[x]$.

- Sea $\alpha \in \overline{\mathbb{Q}}$ una raiz de $p(x)$, y sea $K = \mathbb{Q}(\alpha)$. Muestre que $[K : \mathbb{Q}] = 4$.

  Proof. El polinomio $p(x)$ es irreducible por el criterio de Einsenstein. Luego $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ es igual al grado del polinomio que es cuatro. $\square$

- Se puede mostrar que si L es el cuerpo de descomposición de $p(x)$ sobre K entonces $[L : K] = 3$. Asumiendo lo anterior muestre que $K/\mathbb{Q}$ no tiene sub-extensiones propias no triviales.

  Proof. Las subextensiones no triviales de $K/\mathbb{Q}$ deberian ser de grado 2 y debemos demostrar que estas extensiones no existen. Por torres tendriamos que el cuerpo de descomposición de nuestro polinomio es de grado 12. Sea M una extensión no trivial de K, entonces por torres tendriamos que $[L : M] = 6$. Por lo tanto, el enunciado es equivalente a demostrar que $\text{Gal}\mathbb{Q}$ no tiene subgrupos de orden 6. Por un teorema tenemos que $\text{Gal}(L/\mathbb{Q}) \leq A_4$ si y solo si la raíz del determinante de $p(x)$ pertenece a Q. El discrimante de este polinomio calculado por Wolfram Alpha es $3136 = 56^2$. Por lo tanto, $\text{Gal}(L/\mathbb{Q}) \leq A_4$ pero como $|\text{Gal}(L/\mathbb{Q})| = |A_4| = 12$ concluimos que $\text{Gal}(L/\mathbb{Q}) \cong A_4$. Y en la literatura existe una prueba típica de que A_4 no contiene un subgrupo de orden 6, (suponiendo por contradicción y llegando a la concluisión de que debería contener todos los 3-ciclos que son 8). Por lo tanto, no puede existir una extensión propia no trivial de $K/\mathbb{Q}$. $\square$

6. Sea $L/\mathbb{Q}$ una extensión de Galois y suponga que $\text{Gal}(L/\mathbb{Q}) \cong Q_8$ el grupo de Cuaterniones. (Un ejemplo construido a inicios de los 80 de tal extensión es $L = \mathbb{Q}(\alpha)$ donde α es una raíz de $x^8 - 72x^6 + 180x^4 - 144x^2 + 36$.)

- Muestre que toda sub-extensión $K/\mathbb{Q}$ de $L/\mathbb{Q}$ es de Galois.

  Proof. Esto se sigue del hecho de que en Q_8 todos los subgrupos son normales. Recordemos que en Q_8 los elementos i, j y k tienen orden 4. Como el indice de los grupos de orden 4 es 2 todos estos grupos son normales. Además, el único elemento de orden 2 en Q_8 es -1 y se cumple que $Z(Q_8) = \{1, -1\}$. Por lo tanto, este único subgrupo de orden 2 es normal en Q_8 y esto nos indica que no hay más subgrupos propios que considerar. Por lo tanto, como toda sub-extensión tiene asociada un subgrupo normal,todas las sub-extensiones son normales. $\square$

- Suponga que $K/\mathbb{Q}$ es una sub-extensión cuadrática de $L/\mathbb{Q}$. Muestre que $K \subseteq \mathbb{R}$.

  Proof. Que $K \subseteq \mathbb{R}$ significa que K debe ser invariante bajo conjugación. Entonces el enunciado es equivalente a mostrar que $\phi \in \text{Gal}(L/K)$. donde $\phi(x) = \overline{x}$. Entonces tenemos dos posibilidades, que $\phi(x)|_L = id$ en cuyo caso claramente pertenece a $\text{Gal}(L/K)$ porque la identidad siempre pertenece a cualquier grupo de Galois. La segunda posibilidad es que $\phi(x)|_L \not= id$ y en este caso tendriamos que este elemento estaria asociado al elemento de orden 2, -1 en $\mathbb{Q}_8$. Y si construimos el retículo del grupo ("lattice" en ingles) veriamos que -1 pertenece a todos los subgrupos en $\mathbb{Q}_8$, en particular pertenece a $\text{Gal}(L/K)$ y esto concluye la demostración. $\square$

Productos fibrados de grupos: Recuerde que dados grupos G_1, G_2 y G y morfismos $\phi_i : G_i \to G$ el producto fibrado de G_1 por G_2 sobre G, con respecto a los morfismos ϕ_i, es el subgrupo de $G_1 \times G_2$ definido como

$$G_1 \times_G G_2 := \{(g_1, g_2) \ : \ \phi_1(g_1) = \phi_2(g_2)\}.$$

Por ejemplo si $G = \{e\}$ es el grupo trivial el producto fibrado $G_1 \times_{\{e\}} G_2$ es el producto cartesiano usual.