Soluciones del segundo parcial

Ejercicio 1. Sea p primo y K un cuerpo de característica p. Sea $n \in \mathbb{N}$ tal que $p \mid n$, consideramos $\overline{\Phi_n} \in K[X]$ la reducción módulo p del n-ésimo polinomio ciclotómico. Probar que:

a) $\overline{\Phi_n}$ es separable si y solo si $p = 2$ y $n/2$ es impar.

b) Si p es distinto de 2, entonces $\overline{\Phi_n}$ es reducible.

Solución 1. *a)* $\Leftarrow$) Sea $p = 2$ y $n/2$ impar. Por el ejercicio 4.d de la práctica 6 sabemos que, siendo $n/2$ es impar, se tiene $\Phi_n(X) = \Phi_{n/2}(-X)$. Entonces al hacer la reducción módulo 2 obtenemos $\overline{\Phi_n(X)} = \overline{\Phi_{n/2}}(-X) = \overline{\Phi_{n/2}}(X)$. Como $n/2$ es coprimo con p, tenemos que $\overline{\Phi_{n/2}}$ es separable, por el ejercicio 7.c de la práctica 6.

$\Rightarrow$) Supongamos que $n = p^r \cdots$ donde $s = p_1^{e_1} \dots p_t^{e_t}$ y $r > 1$. Entonces por ejercicio 4.*c* de la práctica 6 tenemos que $\Phi_n(X) = \Phi_{pm}(X^{p^{r-1}e})$ donde $n = p_1 \cdots p_t$ y $e = p_1^{e_1-1} \cdots p_t^{e_t-1}$. Notemos que si ahora reducimos módulo p, entonces $\overline{\Phi_n}(X) = \overline{\Phi_{p\,m}}(X^e)^{p^{r-1}}$ como $r > 1$ esto ya nos dice que $\overline{\Phi_n}$ no es separable.

Por otro lado, ¿Qué pasa si $n = p\,s$ con p coprimo a s? del ejercicio 4.*e* de la misma práctica tenemos que $\Phi_n(X) = \Phi_{p\,s}(X) = \frac{\Phi_s(X^p)}{\Phi_s(X)}$. De esta forma $\Phi_n(X) \cdot \Phi_s(X) = \Phi_s(X^p)$.

Reduciendo módulo p obtenemos $\overline{\Phi}_n(X).\overline{\Phi}_s(X) = \overline{\Phi}_s(X)^p$ de forma que $\overline{\Phi}_n(X) = \overline{\Phi}_s(X)^{p-1}$, lo cual nos dice que $\overline{\Phi}_n(X)$ es no separable a menos que $p = 2$.

b) Supongamos que $p > 2$ y sea $n = p^r s$ con p y s coprimos. Sabemos que $\overline{\Phi_n} \mid (X^s - 1)^{p^r}$ pues $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Si $\overline{\Phi_n}$ fuera irreducible, entonces es primo (pues $K[X]$ DFU) y por lo tanto $\overline{\Phi_n} \mid X^s - 1$. Pero $X^s - 1$ es separable, por lo tanto $\overline{\Phi_n}$ sería separable pero esto es absurdo por el item anterior.

□

Ejercicio 2. Sea K una extensión finita de $\mathbb{F}_q$.

a) Probar que $Tr_{K/\mathbb{F}_q}(\alpha^q) = Tr_{K/\mathbb{F}_q}(\alpha)$ para todo $\alpha \in K$.

b) Deducir que $Tr_{K/\mathbb{F}_q}(\alpha) = 0$ sii el polinomio $X^q - X - \alpha$ tiene una raíz en K.

Solución 2. *a)* Sea $G = Gal(\mathbb{F}_{q^s}/\mathbb{F}_q)$ Consideremos el automorfismo $Frob_q : x \mapsto x^q \in G$. Como $K/\mathbb{F}_q$ es separable, tenemos

$$Tr_{K/\mathbb{F}_q}(\alpha^q) = Tr_{K/\mathbb{F}_q}(Frob_q(\alpha)) = \sum_{\sigma \in G} \sigma(Frob_q(\alpha)) = \sum_{\sigma \in G} \sigma(\alpha) = Tr_{K/\mathbb{F}_q}(\alpha)$$

porque lo único que hace componer con un elemento de G es permutar el orden de sumación, ya que son automorfismos y estamos sumando sobre todos ellos.

b) $\Rightarrow$) Si $Tr_{K/\mathbb{F}_q}(\alpha) = 0$, como G está generado por $Frob_q$, por Teorema 90 de Hilbert (versión aditiva), existe $z \in K$ con $\alpha = Frob_q(z) - z = z^q - z$. Por lo tanto $z^q - z - \alpha = 0$ con lo cual el polinomio $X^q - X - \alpha$ tiene una raíz en K.

$\Leftarrow$) Reciprocamente, si $X^q - X - \alpha$ tiene una raíz $z \in K$, tenemos que $z^q - z - \alpha = 0$. Tomando traza a esta expresión resulta que, por la aditividad,

$$Tr_{K/\mathbb{F}_q}(z^q) - Tr_{K/\mathbb{F}_q}(z) - Tr_{K/\mathbb{F}_q}(\alpha) = 0,$$

y por el ítem anterior tenemos que $Tr_{K/\mathbb{F}_q}(\alpha) = 0$ como queríamos.

□

Ejercicio 3. Sea $f \in \mathbb{Q}[X]$ polinomio irreducible de grado 7 resoluble por radicales. Probar que si $\Delta(f) < 0$ entonces f tiene exactamente una raíz real.

Solución 3. Para empezar, notemos que como el polinomio es irreducible, es separable, y por lo tanto su discriminante es no nulo.

Notemos que el polinomio no puede tener todas raíces reales porque si no su discriminante sería positivo al ser un producto de cuadrados de números reales. Luego tiene al menos una raíz no real. La cantidad de raíces no reales es par, por tratarse de un polinomio con coeficientes en $\mathbb{R}$.

No puede tener sólo dos raíces no reales pues vimos en un ejercicio de la práctica 7 que si un polinomio en $\mathbb{Q}[X]$ es de grado primo p, irreducible y tiene exactamente 2 raíces no reales entonces su grupo de Galois es S_p. Como S_7 no es un grupo soluble, esto nos llevaría a un absurdo.

Por lo tanto, resta descartar el caso en el que f tiene 4 raíces no reales. Veamos que en este caso el discriminante nos daría positivo.

Para eso, consideremos a_1, a_2 y a_3 las raíces reales y sean b_1, $\overline{b_1}$,b_2 y $\overline{b_2}$ las 4 raíces no reales. Entonces agrupando los factores de $\Delta(f)$ convenientemente tenemos:

- $\prod_{1 \le i < j \le 3}(a_i - a_j)^2 > 0$, pues $a_i - a_j \in \mathbb{R}$
- $(b_1 - \overline{b_1})^2(b_2 - \overline{b_2})^2 > 0$, pues $b_i - \overline{b_i} \in i\mathbb{R}$
- $(b_1 - b_2)^2(\overline{b_1} - \overline{b_2})^2 > 0$, pues $(b_1 - b_2)(\overline{b_1} - \overline{b_2}) = |b_1 - b_2|^2$.
- $(b_1 - \overline{b_2})^2(b_2 - \overline{b_1})^2 > 0$, como en el ítem anterior.
- $(a_i - b_j)^2(a_i - \overline{b_j})^2 > 0$ para $1 \le i \le 3$, $1 \le j \le 2$, como en el ítem anterior.

□

Ejercicio 4. Dados un anillo C y un ideal primo $P \subseteq B$ definimos la altura de P como:

$$h(P) = \sup\{n \ge 0 : \text{ existen primos } P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = P\}$$

Sean $A \subseteq B$ anillos tales que para todo $x \in B$ existe $n \ge 1$ tal que $x^n \in A$.

a) Probar que para todo ideal primo $p \subseteq A$ existe un único ideal primo $\mathcal{B} \subseteq B$ tal que $\mathcal{B} \cap A = p$.

b) Probar que $h(p) = h(\mathcal{B})$.

Solución 4. *a*) Veamos primero que B es entero sobre A. Dado $x \in B$, por hipótesis existe $n \geq 1$ tal que $x^n \in A$. Luego $T^n - x^n \in A[T]$ es un polinomio mónico que anula a x, por lo que B es entero sobre A.

Vimos en clase que si B es entero sobre A, entonces dado un ideal primo $p \subseteq A$ existe un ideal primo $\mathcal{P} \subseteq B$ tal que $A \cap \mathcal{P} = p$.

Solo queda ver que es único. Sean $\mathcal{P}_1, \mathcal{P}_2 \subseteq B$ ideales primos tales que $\mathcal{P}_1 \cap A = p$ y $\mathcal{P}_2 \cap A = p$. Veamos que $\mathcal{P}_1 = \mathcal{P}_2$. Sea $b_1 \in \mathcal{P}_1$, entonces existe n tal que $b_1^n \in A$. Pero entonces $b_1^n \in \mathcal{P}_1 \cap A = p = \mathcal{P}_2 \cap A$ y por lo tanto $b_1^n \in \mathcal{P}_2$. Como $\mathcal{P}_2$ es primo resulta que $b_1 \in \mathcal{P}_2$.

El mismo argumento prueba que $\mathcal{P}_2 \subseteq \mathcal{P}_1$.

b) Sea $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = p$ una cadena de ideales primos de A. Por el teorema del Going-up, existen $\mathcal{P}_0 \subsetneq \mathcal{P}_1 \subsetneq \cdots \subseteq \mathcal{P}_n$ ideales primos de B tales que $A \cap \mathcal{P}_i = P_i$. Notemos que por la unicidad probada en el ítem anterior, debe ser $\mathcal{P}_n = P$. Ahora queremos ver que las inclusiones $\mathcal{P}_i \subseteq \mathcal{P}_{i+1}$ son estrictas. Si $\mathcal{P}_i = \mathcal{P}_{i+1}$, entonces $P_i = \mathcal{P}_i \cap A = \mathcal{P}_{i+1} \cap A = P_{i+1}$, pero $P_i \subsetneq P_{i+1}$. Luego probamos que $h(p) \leq h(\mathcal{B})$.

Para el otro lado, si tenemos una cadena $\mathcal{P}_0 \subsetneq \mathcal{P}_1 \subsetneq \cdots \subsetneq \mathcal{P}_n = \mathcal{B}$ de ideales primos de B, entonces es claro que $\mathcal{P}_i \cap A = P_i$ son ideales primos de A. Veamos que las inclusiones $P_i \subseteq P_{i+1}$ son estrictas. Supongamos que $P_i = P_{i+1}$ para algún i. Entonces $P_i = \mathcal{P}_i \cap A = \mathcal{P}_{i+1} \cap A = P_{i+1}$, pero por la unicidad probada en el punto anterior tendriamos que $\mathcal{P}_i = \mathcal{P}_{i+1}$, lo cual es absurdo porque las contenciones eran estrictas. Concluimos que $h(\mathcal{B}) \leq h(p)$.

Luego $h(p) = h(\mathcal{B})$ como queríamos.

□

Ejercicio 5. Sean p y q primos distintos, y sea $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$

a) Sea $\alpha \in K$. Probar que α es un entero algebraico si y solo si $Tr_{K/\mathbb{Q}(\sqrt{p})}(\alpha)$ y $N_{K/\mathbb{Q}(\sqrt{p})}(\alpha)$ lo son.

b) Supongamos que $p \equiv 3 \mod 4$. Probar que si $\alpha \in K$ es un entero algebraico, existen $a, b, c, d \in \mathbb{Z}$ tales que $\alpha = 1/2(a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq})$

Solución 5. Para empezar, notemos que $Gal(K/\mathbb{Q}(\sqrt{p})) = \{Id, \sigma\}$ donde $\sigma : \sqrt{q} \mapsto -\sqrt{q}$ y $\sqrt{p}$ queda quieto.

a) $\Rightarrow$) ¿Es $\sigma(\alpha)$ entero sobre $\mathbb{Z}$? Sí, pues $\sigma \in Gal(K/\mathbb{Q})$, y por lo tanto $\sigma(\alpha)$ es raíz del polinomio mónico en $\mathbb{Z}[X]$ que anule a α.

Como los enteros sobre $\mathbb{Z}$ forman un anillo, resulta que $Tr_{K/\mathbb{Q}(\sqrt{p})}(\alpha) = \alpha + \sigma(\alpha)$ es entero sobre $\mathbb{Z}$, y también lo es $N_{K/\mathbb{Q}(\sqrt{p})}(\alpha) = \alpha \cdot \sigma(\alpha)$.

$\Leftarrow$) Recordemos que si tenemos $A \subseteq B \subseteq C$ anillos, si B es entero sobre A y C es entero sobre B, entonces C es entero sobre A.

En nuestro caso notemos que el polinomio $X^2 - Tr_{K/\mathbb{Q}(\sqrt{p})}X + N_{K/\mathbb{Q}(\sqrt{p})} \in \mathcal{O}_K[X]$ anula a α, luego α es entero sobre el anillo $\mathcal{O}_K$. Pero $\mathcal{O}_K$ es entero sobre $\mathbb{Z}$, entonces por la transitividad α es entero en $\mathbb{Z}$.

b) Escribamos $\alpha = A + B\sqrt{p} + C\sqrt{q} + D\sqrt{pq}$, con $A, B, C, D \in \mathbb{Q}$.

Por el item anterior resulta que $Tr_{K/\mathbb{Q}(\sqrt{p})}(\alpha) = \alpha + \sigma(\alpha) = 2A + 2B\sqrt{p} \in \mathcal{O}_{\mathbb{Q}(\sqrt{p})}$.

Dado que $Gal(K/\mathbb{Q}(\sqrt{q})) = \{1, \sigma\}$ donde $\sigma : \sqrt{p} \mapsto -\sqrt{p}$, tenemos análogamente que $Tr_{K/\mathbb{Q}(\sqrt{q})}(\alpha) = \alpha + \sigma(\alpha) = 2A + 2C\sqrt{q} \in \mathcal{O}_{\mathbb{Q}(\sqrt{q})}$.

Por último, dado que $Gal(K/\mathbb{Q}(\sqrt{pq})) = \{1, \sigma\}$ donde $\sigma : \sqrt{p} \mapsto -\sqrt{p}$, obtenemos que $Tr_{K/\mathbb{Q}(\sqrt{qp})}(\alpha) = 2A + 2D \in \mathcal{O}_{\mathbb{Q}(\sqrt{pq})}$.

En resumen obtuvimos:

(a) $2A + 2B\sqrt{p} \in \mathcal{O}_{\mathbb{Q}(\sqrt{p})}$

(b) $2A + 2C\sqrt{q} \in \mathcal{O}_{\mathbb{Q}(\sqrt{q})}$

(c) $2A + 2D\sqrt{pq} \in \mathcal{O}_{\mathbb{Q}(\sqrt{pq})}$

En lo que sigue haremos uso del ejercicio 19 de la práctica 8.

Notemos que por este ejercicio sabemos que $2A, 2B \in \mathbb{Z}$ pues $p \equiv 3 \mod 4$. Por lo tanto $2A = a$ con $a \in \mathbb{Z}$, luego $A = \frac{1}{2}a$. Lo mismo pasa con B, sabemos que existe $b \in \mathbb{Z}$ tal que $B = \frac{1}{2}b$.

Ahora, escribimos $2A + 2C = (4A + 4C)/2$. Por el ejercicio 18, sea quien sea q sabemos que $4A, 4C \in \mathbb{Z}$ y son congruentes módulo 2. Como $2A \in \mathbb{Z}$, $4A$ es par con lo cual $4C$ es par y por ende $2C \in \mathbb{Z}$. Esto es, existe $c \in \mathbb{Z}$ tal que $C = \frac{1}{2}c$.

De forma enteramente análoga vale que que $D = \frac{1}{2}d$ con $d \in \mathbb{Z}$.

□