Examen parcial 2 - soluciones

(3 nov, 2010)

1. (20 pts) Sea $f(x)$ un polinomio con coeficientes en un campo F.

   a) (2 pts) Define: un campo de descomposición para $f(x)$.

   ▷ Es una extensión K/F tal que $f(x)$ se factoriza en factores lineales en $K[x]$ y tal que K está generado por las raices de $f(x)$ en K.

   b) (8 pts) Demuestra: existe un campo de descomposición para $f(x)$.

   ▷ Por inducción sobre el grado de $f(x)$: para grado 1 no hay nada que demostrar (F mismo es un campo de descomposición de $f(x)$). Para el caso general, sea $g(x)$ un factor irreducible de $f(x)$. Luego $F_1 = F[x]/(g(x))$ es una extensión de F en donde hay una raíz de $g(x)$ (la clase de x), la cual es una raíz de $f(x)$. Así que $f(x)$ tiene un factor lineal en F_1, o sea $f(x) = (x-\alpha)f_1(x)$. Aplicando inducción a $f_1(x)$ (tiene un grado menor que $f(x)$), hay una extensión K de F_1 en donde $f_1(x)$ se descompone en factores lineals. □

   c) (10 pts) Demuestra: dadas dos extensiones K/F, K'/F, tal que K, K' son campos de descomposición para $f(x)$, existe un isomorfismo de campos $K \to K'$ cuya restricción a F es la identidad.

   ▷ Primero un lema: sea $\phi : F \to \tilde{F}$ un ismorfismo de campos y K/F, $\tilde{K}/\tilde{F}$ extensiones de campos. Sea $g(x) \in F[x]$ un polinomio irreducible y $\tilde{g}(x) \in \tilde{F}(x)$ la imagen de $g(x)$ bajo ϕ (se aplica ϕ a los coeficientes de $g(x)$). Sea $\alpha \in K$ (resp. $\tilde{\alpha} \in \tilde{F}$) una raíz de $g(x)$ (resp. $\tilde{g}(x)$). Entonces ϕ se extiende a un isomorfismo $F(\alpha) \to \tilde{F}(\tilde{\alpha})$.

   Idea de la demostración del lema: como $g(x)$ es irreducible, $F(\alpha)$ es isomorfo canónicamente a $F[x]/(g(x))$ y analógamente $\tilde{F}(\tilde{\alpha}) \cong \tilde{F}[x]/(\tilde{g}(x))$. Luego ϕ induce un ismorfismo $F[x]/(g(x)) \cong \tilde{F}[x]/(\tilde{g}(x))$.

   Ahora demostramos por inducción sobre el grado de K/F algo un poco más fuerte de lo que se pide: sea $\phi : F \to \tilde{F}$ un isomorfismo de campos, $f(x) \in F[x]$ y $\tilde{f}(x) \in \tilde{F}[x]$ la imagen de $f(x)$ bajo ϕ. Sea K (resp. $\tilde{K}$) un campo de descomposición de $f(x)$ (resp. $\tilde{f}(x)$). Entonces existe una extensión de ϕ a un ismorfismo $K \to \tilde{K}$.

   Si $[K : F] = 1$ no hay nada que demostrar ($F = K$, $\tilde{F} = \tilde{K}$.) Para el caso general, sea $g(x) \in F[x]$ un factor irreducible de $f(x)$ de grado > 1, $\tilde{g}(x) \in \tilde{F}[x]$ la imagen de $g(x)$ bajo ϕ, $\alpha \in K$ una raíz de $g(x)$ y $\tilde{\alpha} \in \tilde{K}$ una raíz de $\tilde{g}(x)$. Entonces según el lema, ϕ se extiende a un isomorfismo $F(\alpha) \to \tilde{F}(\tilde{\alpha})$. Luego K (resp. $\tilde{K}$) es un campo de descomposición para $f(x)$ (resp. $\tilde{f}(x)$) sobre $F(\alpha)$ (resp. $\tilde{F}(\tilde{\alpha})$) y $[K : F(\alpha)] = [K : F]/[F(\alpha) : F] < [K : F]$, así que por inducción se extiende el isomorfismo $F(\alpha) \to \tilde{F}(\tilde{\alpha})$ a un ismorfismo $K \to \tilde{K}$. □

2. (80 pts) Sea $f(x) = x^5 - 2 \in \mathbb{Q}[x]$ y sea $K = \mathbb{Q}(\alpha, \omega) \subset \mathbb{C}$, donde $\alpha = \sqrt[5]{2}$ y $\omega = e^{2\pi i/5}$.

a) (2 pts) Demuestra que $f(x)$ es irreducible.

▷ Aplicamos el criterio de Eisenstein en el primo $p = 2$. □

b) (3 pts) Demuestra que K es un campo de descomposición para $f(x)$.

▷ K contiene las 5 raices $\alpha\omega^i$, $i = 0, 1, 2, 3, 4$ así que $f(x)$ se factoriza en factores lineales en K. Luego ω es el cociente de las primeras dos raices así que ω está en el campo generado por las raices, por lo que K está generado por las 5 raices.

c) (5 pts) Demuestra que $\mathbb{Q}(\omega)/\mathbb{Q}$ es una extensión de Galois de grado 4, cuyo grupo de Galois es isomorfo a $\mathbb{Z}_4$.

▷ $\mathbb{Q}(\omega)$ es un campo de descomposición de x^5-1 (las raices de este son potencias de ω) por lo que es una extensión de Galois. El polinomio irreducible de ω es $(x^5-1)/(x-1)$, por lo que $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$. Luego para cada $i = 1, 2, 3, 4$ existe un automorfismo único de $\mathbb{Q}(\omega)$ tal que $\omega \to \omega^i$; tal automorfismo existe ya que sabemos que ω, ω^i son dos raices del mismo polinomio irreducible y generan el mismo subcampo de $\mathbb{C}$. Sea entonces ϕ el automorfismo de $\mathbb{Q}(\omega)$ dado por $\phi(\omega) = \omega^2$. Es fácil calcular que $\phi^k(\omega) = \omega^{2^k}$, y de aquí, que ϕ tiene orden 4. □

d) (5 pts) Encuentra todos los subcampos de $\mathbb{Q}(\omega)$.

▷ Estos son los subcampos fijos de subgrupos del grupo de Galois. Como el grupo es cíclico, generado por ϕ, los subgrupos tambien son cíclicos, generados por ϕ^d, donde d es un divisor del orden de ϕ. Estos son $d = 1, 2, 4$. Para $d = 1$ el subcampo es $\mathbb{Q}$, para $d = 4$ es todo $\mathbb{Q}(\omega)$ y para $d = 2$ el subcampo es de grado 2 así que está generado por un elemento cudrático, fijo por ϕ^2. Ahora $\phi^2(\omega) = \omega^4$, así que $\omega + \omega^4 = 2\cos(2\pi/5)$ genera el subcampo buscado. □

e) (5 pts) Demuestra que $\mathbb{Q}(\alpha)/\mathbb{Q}$ es una extensión de grado 5 cuyo grupo de Galois es trivial, por lo que no es una extensión de Galois.

▷ α tiene polinomio irreducible $f(x)$ de grado 5 (inciso (a)), por lo que genera una extensión de grado 5. Caulquer automorfismo del campo generado por α debe mandar α a otra raiz de $f(x)$, pero los demas raices son complejas, mientras α genera un campo real, por lo que el único auntomorfismo de $\mathbb{Q}(\alpha)$ es la identidad. En particular, la extensión no es Galois $\mathbb{Q}(\alpha)/\mathbb{Q}$ (su grupo de Galois tiene menos elementos que su grado).

f) (5 pts) Encuentra todos los subcampos de $\mathbb{Q}(\alpha)$.

▷ Como la extensión no es de Galois, el teorema fundamental no nos ayuda. Pero usando que $\mathbb{Q}(\alpha)/\mathbb{Q}$ tiene grado 5, un primo, no tiene subcampos mas que $\mathbb{Q}(\alpha)$ y $\mathbb{Q}$.

g) (5 pts) Encuentra el grado de la extensión $K/\mathbb{Q}$.

▷ K tienes dos subcampos, $\mathbb{Q}(\alpha)$ y $\mathbb{Q}(\omega)$, de grados 5 y 4 (resp.) sobre $\mathbb{Q}$, por lo que el grado de $K/\mathbb{Q}$ es un múltiplo de ambos 4 y 5, o sea múltiplo de 20. Por otro lado ω tiene grado 4 sobre $\mathbb{Q}$, por lo que tiene grado ≤ 4 sobre $\mathbb{Q}(\alpha)$, así que K tiene grado $\leq 4 \cdot 5 = 20$ sobre $\mathbb{Q}$. En conclusión, $[K : \mathbb{Q}] = 20$. □

h) (45 pts) Sea G el grupo de Galois de $K/\mathbb{Q}$. ¿Qué puedes concluir de los incisos anteriores acerca del grupo G?

Sugerencias: G es isomorfo a un subgrupo de S_5 de orden 20, actuando transitivamente en $\{1,2,3,4,5\}$; G contiene un subgrupo normal N isomorfo a $\mathbb{Z}_5$ tal que G/N es isomorfo a $\mathbb{Z}_4$; G contiene un subgrupo de orden 4 que no es normal, por lo que G no es abeliano.

▷ El grupo de Galois de una ecuación irreducible $f(x) \in F[x]$ actua trasitivamente en el conjunto de las raices de la ecuación (en un campo de descomposision). Demostración: sea K una campo de descomposición de $f(x)$. Dados dos raices, $\alpha, \alpha' \in K$ existe un isomorfismo $F(\alpha) \to F(\alpha')$ que manda $\alpha \to \alpha'$ (ver problema anterior). Ahora K es un campo de descomposición para $f(x)$ sobre ambos $F(\alpha), F(\alpha')$ por lo que el isomorfismo $F(\alpha) \to F(\alpha')$ se extiende a un isomorfismo (automorfismo) $K \to K$.

Como $\mathbb{Q}(\omega)/\mathbb{Q}$ es una extensión de Galois de grado 4, el subgrupo correspondiente $N \subset G$ es normal y de grado 5, por lo que es isomorfo a $\mathbb{Z}_5$. El cociente G/N es el grupo de Galois de $\mathbb{Q}(\omega)/\mathbb{Q}$ por lo que es isomporfo a $\mathbb{Z}_4$.
Como $\mathbb{Q}(\alpha)/\mathbb{Q}$ es de grado 5 y no es de Galois, el subgrupo correspondiente $H \subset G$ es de grado 4 y no es normal, por lo que G no es abeliano. □

i) Extra crédito (opcional): determina a G como un subgrupo de S_5 (el grupo de permutaciones de las raices de $f(x)$), encuentra a todos los subgrupos de G y los subcampos de K.