Universidad del Valle de Guatemala
Departamento de Matemática
Licenciatura en Matemática Aplicada

Estudiante: Rudik Roberto Rompich
Correo: rom19857@uvg.edu.gt
Carné: 19857

MM2035 - Álgebra Moderna - Catedrático: Ricardo Barrientos
1 de diciembre de 2022

Tarea 24

Problemas 1, 2, 3, 4, 5, 6, 8, 12 y 17, sección 5.6

Problema 1 (Problema 1)**.** *If K is a field and S a set of automorphisms of K, prove that the fixed field of S and that of $\bar{S}$ (the subgroup of the group of all automorphisms of K generated by S) are identical.*

Demostración. Sea el campo fijado de S definido como $K_1 = \{k \in K : \sigma(k) = k, \forall \sigma \in S\}$ y el campo fijado de $\overline{S}$ definido como $K_2 = \{k \in K : \sigma(k) = k, \forall \sigma \in \overline{S}\}$. A probar: $K_1 = K_2$. Entonces,

- ($\supseteq$) Sea $z \in K_2 \implies \sigma(z) = z, \forall z \in \overline{S} \implies$ como $\overline{S}$ es el subgrupo de todos los automorfismos de K generados por $S \implies \sigma(z) = z, \forall \sigma \in S \implies z \in K_1$. Por lo tanto, $K_1 \supseteq K_2$.
- ($\subseteq$) Sea $z \in K_1 \implies \sigma(z) = z, \forall z \in S$. Por otra parte, como $\overline{S}$ está generado por S, un elemento de $\overline{S}$ puede ser escrito como la multiplicación de elementos de S, sea $\delta \in \overline{S} \implies \delta = \sigma_1\sigma_2\sigma_3 \cdots \sigma_n$, evaluando en z, $\delta(z) = \sigma_1\sigma_2\sigma_3 \cdots \sigma_n(z) = z$ debido a que ya sabíamos que $\sigma(z) = z, \forall \sigma \in S \implies z \in K_2$. Por lo tanto, $K_1 \subseteq K_2$.

Por lo tanto, $K_1 = K_2$. ■

Problema 2 (Problema 2)**.** *Prove Lemma 5.6.2.*

El lema 5.6.2 es el lema 5.8 demostrado en clase, el cual dice:

Si F es un campo y K es una extensión de F , entonces, $G(K, F)$ es un subgrupo de $\mathbb{A}(K)$.

Demostración. Si $\sigma_1, \sigma_2 \in G(K, F) \implies$ si $\alpha \in F, \sigma_1\sigma_2(\alpha) = \sigma_2(\sigma_1(\alpha)) \underbrace{=}_{\sigma_1 \in G(K,F)} = \sigma_2(\alpha) \underbrace{=}_{\sigma_2 \in G(K,F)} \alpha \implies \sigma_1\sigma_2 \in G(K, F)$. Si $\sigma \in G(K, F)$ y $\alpha \in F \implies \sigma(\alpha) = \alpha, \forall \alpha \in F \implies \sigma^{-1}(\alpha) = \sigma^{-1}(\sigma(\alpha)) = \sigma\sigma^{-1}(\alpha) = I_k(\alpha) = \alpha \implies \sigma^{-1} \in G(K, F)$. Por el lema 2.3, $G(K, F)$ es subgrupo de $\mathbb{A}(K)$. ■

Problema 3 (Problema 3)**.** *Using the Eisenstein criterion, prove that* $x^4+x^3+x^2+x+1$ *is irreducible over the field of rational numbers.*

Demostración. A probar: $f(x) = x^4+x^3+x^2+x+1$ es irreducible sobre los racionales. En una tarea previa, se había demostrado que $f(x)$ es irreducible si y solo si $f(x+1)$ también es irreducible. Entonces,

$$\begin{aligned}
f(x+1) &= (x+1)^4 + (x+1)^3 + (x+1)^2 + (x+1) + 1 \\
&= (x+1)^2(x+1)^2 + (x+1)^2(x+1) + (x+1)^2 + (x+1) + 1 \\
&= (x+1)^2((x+1)^2 + (x+1) + 1) + (x+1) + 1 \\
&= (x^2+2x+1)(x^2+2x+1+x+1+1) + (x+1) + 1 \\
&= (x^2+2x+1)(x^2+3x+3) + (x+1) + 1 \\
&= x^4 + 3x^3 + 3x^2 + 2x^3 + 6x^2 + 6x + x^2 + 3x + 3 + (x+1) + 1 \\
&= x^4 + 5x^3 + 10x^2 + 10x + 5
\end{aligned}$$

Entonces, aplicando el criterio de Eisenstein para el primo $p=5$, $p \not| 1$ pero sí es divisor de los demás coeficientes, entonces se cumple que $f(x)$ es irreducible. ■

Problema 4 (Problema 4)**.** *In Example 5.6.3, prove that each mapping* σ_i *defined is an automorphism of* $\mathbb{Q}(\omega)$*.*

Demostración. Este ejemplo se resolvió en clase, en donde el propósito era encontrar $G(\mathbb{Q}(e^{2\pi i/5}), \mathbb{Q})$. Se tiene que $\omega = e^{2\pi i/5}$ son raíces de $f(x) = x^4+x^3+x^2+x+1$ y que es irreducible por el **Problema 3** en $\mathbb{Q} \implies [\mathbb{Q}(\omega) : \mathbb{Q}] = 4 \implies \mathbb{Q}(\omega) = \{\alpha_0 + \alpha_1\omega + \alpha_3\omega^2 + \alpha_3\omega^2 \quad \alpha_0, \alpha_1, \alpha_3, \alpha_3 \in \mathbb{Q}\}$. Si $\sigma \in G(\mathbb{Q}(\omega), \mathbb{Q}) \Rightarrow \sigma(\omega) \neq 1$ y $1 = \sigma(1) = \sigma(\omega^5) = \sigma(\omega)^5$. Sean $\sigma_2(\omega) = \omega^2, \sigma_3(\omega) = \omega^3, \sigma_4(\omega) = \omega^4$, entonces:

$$\begin{aligned}
\sigma_i\left(\alpha_0 + \alpha_1\omega + \alpha_2\omega^2 + \alpha_3\omega^3\right) &= \sigma_i(\alpha_0) + \sigma_i(\alpha_1)\sigma_i(\omega) + \sigma_i(\alpha_2)\sigma_i\left(\omega^2\right) + \sigma_i(\alpha_3)\sigma_i\left(\omega^3\right) \\
&= \alpha_0 + \alpha_1\omega^2 + \alpha_2(\sigma_i(\omega))^2 + \alpha_3(\sigma_i(\omega))^3 \\
&= \alpha_0 + \alpha_1\omega^i + \alpha_2(\omega^i)^2 + \alpha_3(\omega^i)^3
\end{aligned}$$

De esto, se obtenía lo siguiente:

- $i=1$:

$$\sigma_1\left(\alpha_0 + \alpha_1\omega + \alpha_2\omega^2 + \alpha_3\omega^3\right) = \alpha_0 + \alpha_1\omega^1 + \alpha_2(\omega)^2 + \alpha_3(\omega)^3$$

  Entonces σ_1 es un automorfismo de $\mathbb{Q}(\omega)$.

- $i=2$:

$$\begin{aligned}
\sigma_2\left(\alpha_0 + \alpha_1\omega + \alpha_2\omega^2 + \alpha_3\omega^3\right) &= \alpha_0 + \alpha_3\omega + \alpha_1\omega^2 + \alpha_2\omega^4 \\
&= \alpha_0 + \alpha_3\omega + \alpha_1\omega^2 + \alpha_2(-\omega^3 - \omega^2 - \omega - 1) \\
&= (\alpha_0 - \alpha_2) + (\alpha_3 - \alpha_2)\omega + (\alpha_1 - \alpha_2)\omega^2 - \alpha_2 w^3
\end{aligned}$$

  En el problema 4, se concluye que $\alpha_1 = \alpha_2 = \alpha_3 = 0$, lo que nos permite concluir:

$$= \alpha_0 + \alpha_1\omega + \alpha_2\omega^2 + \alpha_3\omega^3$$

  Entonces σ_1 es un automorfismo de $\mathbb{Q}(\omega)$.

- $i = 3$:

$$\begin{aligned}\sigma_3\left(\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3\right) &= \alpha_0+\alpha_1\omega^3+\alpha_2\omega+\alpha_3(-\omega^3-\omega^2-\omega-1)\\ &= (\alpha_0-\alpha_3)+(\alpha_2-\alpha_3)\omega-\alpha_3\omega^2+(\alpha_1-\alpha_3)\omega^3\end{aligned}$$

En el problema 4, se concluye que $\alpha_1=\alpha_2=\alpha_3=0$, lo que nos permite concluir:

$$= \alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3$$

Entonces σ_1 es un automorfismo de $\mathbb{Q}(\omega)$.

- $i = 4$:

$$\begin{aligned}\sigma_4\left(\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3\right) &= \alpha_0+\alpha_1(-\omega^3-\omega^2-\omega-1)+\alpha_2\omega^3+\alpha_3\omega^2\\ &= (\alpha_2-\alpha_1)-\alpha_1\omega+(\alpha_3-\alpha_1)\omega^2+(\alpha_2-\alpha_1)\omega^3\end{aligned}$$

En el problema 4, se concluye que $\alpha_1=\alpha_2=\alpha_3=0$, lo que nos permite concluir:

$$= \alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3$$

Entonces σ_1 es un automorfismo de $\mathbb{Q}(\omega)$.

■

Problema 5 (Problema 5)**.** *In Example 5.6.3, prove that the fixed field of $\mathbb{Q}(\omega)$ under σ_1, $\sigma_2,\sigma_3,\sigma_4$ is precisely $\mathbb{Q}$.*

Demostración. Continuando con la deducción del **Problema 4**, se tiene:

$$\begin{aligned}&\sigma_2^2(\omega)=\sigma_2(\sigma_2(\omega))=\sigma_2(\omega^2)=\omega^4=\sigma_4(\omega) \implies \sigma_2^2=\sigma_4\\ &\sigma_2^3(\omega)=\sigma_2(\sigma_2^2(\omega))=\sigma_2(\sigma_4(\omega))=\sigma_2(\omega^4)=\omega^3=\omega^2=\sigma_3(\omega) \implies \sigma_2^3=\sigma_3\\ &\sigma_2^4(\omega)=\sigma_2^2(\sigma_2^2(\omega))=\sigma_4(\sigma_4(\omega))=\sigma_3(\omega^4)=\omega^16=\omega=\sigma_1(\omega) \implies \sigma_2^4=\sigma_1\end{aligned}$$

Entonces, $G(\mathbb{Q}(\omega),\mathbb{Q})=(\sigma_2)$ y $o(G(\mathbb{Q}(\omega),\mathbb{Q}))=4$. Si $\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3$ pertenece al subcampo de $\mathbb{Q}$ fijado por $G(\mathbb{Q}(\omega),\mathbb{Q}) \implies \alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3=(\alpha_0-\alpha_3)+(\alpha_2-\alpha_3)\omega=\alpha_3\omega^2+(\alpha_1-\alpha_2)\omega^3=(\omega_0-\omega_1)-\alpha_1\omega+(\alpha_3-\alpha_1)\omega^2+(\alpha_2-\alpha_1)\omega^3$. Entonces,

$$\begin{aligned}\alpha_0&=\alpha_0-\alpha_1=\alpha_0-\alpha_3=\alpha_0-\alpha_1\\ \alpha_1&=\alpha_3-\alpha_2=\alpha_2-\alpha_3=-\alpha_1\\ \alpha_2&=\alpha_1-\alpha_2=-\alpha_3=\alpha_3-\alpha_1\\ \alpha_3&=-\alpha_2=\alpha_1-\alpha_3=\alpha_2-\alpha_1\end{aligned}$$

Entonces $\alpha_1=\alpha_2=\alpha_3=0$. Por lo tanto, el subcampo de $\mathbb{Q}(w)$ fijado por $G(\mathbb{Q}(\omega),\mathbb{Q}) = \mathbb{Q}$ ■

Problema 6 (Problema 6)**.** *Prove directly that any automorphism of K must leave every rational number fixed.*

Demostración. Sea σ un automorfismo cualquiera de K, en donde debemos demostrar que $\sigma : K \to K \ni \sigma(z) = z, \forall z \in \mathbb{Q}$. Entonces, sea $p \in \mathbb{Z}$ y $q \in \mathbb{Z} - \{0\}$, tal que:

$$\begin{aligned}
\sigma\left(\frac{p}{q}\right) &= \sigma(p) \cdot \sigma\left(\frac{1}{q}\right) \\
&= \frac{\sigma(p) \cdot \sigma(1)}{\sigma(q)} \\
&= \frac{p \cdot 1}{q} \\
&= \frac{p}{q} \in \mathbb{Q}
\end{aligned}$$

■

Problema 7 (Problema 8)**.** *Express the following as polynomials in the elementary symmetric functions in x_1, x_2, x_3 :*

Para $n = 3$, las funciones elementales simétricas son:

- $e_1(x_1, x_2, x_3) = x_1 + x_2 + x_3$
- $e_2(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3$
- $e_3(x_1, x_2, x_3) = x_1x_2x_3$

1. $x_1^2 + x_2^2 + x_3^2$.

Solución. Ya que cada una de las variables está al cuadrado, elevar al cuadrado e_1 sería la única opción para obtener las variables al cuadrado:

$$\begin{aligned}
(e_1)^2 &= (x_1 + x_2 + x_3)^2 \\
&= x_1^2 + 2x_2x_1 + 2x_3x_1 + x_2^2 + x_3^2 + 2x_2x_3 \\
&= x_1^2 + x_2^2 + x_3^2 + 2(x_2x_1 + x_3x_1 + x_2x_3) \\
&= x_1^2 + x_2^2 + x_3^2 + 2(e_2)
\end{aligned}$$

Por lo tanto, al despejar

$$x_1^2 + x_2^2 + x_3^2 = (e_1)^2 - 2(e_2)$$

□

2. $x_1^3 + x_2^3 + x_3^3$.

Solución. Mismo procedimiento que el inciso anterior,

$$
\begin{aligned}
(e_1)^3 &= (x_1 + x_2 + x_3)^3 \\
&= (x_1 + x_2 + x_3)(x_1 + x_2 + x_3)^2 \\
&= (x_1 + x_2 + x_3)(x_1^2 + 2x_2x_1 + 2x_3x_1 + x_2^2 + x_3^2 + 2x_2x_3) \\
&= x_1^3 + x_2^3 + x_3^3 + 3x_2x_1^2 + 3x_3x_1^2 + 3x_2^2x_1 + 3x_3^2x_1 + 3x_2x_3^2 + 3x_2^2x_3 + 6x_2x_3x_1 + \\
&+ 3x_2x_3x_1 - 3x_2x_3x_1 \\
&= x_1^3 + x_2^3 + x_3^3 + 3(x_2x_1^2 + x_3x_1^2 + x_2^2x_1 + x_3^2x_1 + x_2x_3^2 + x_2^2x_3 + x_2x_3x_1 + \\
&+ x_2x_3x_1 + x_2x_3x_1) - 3x_2x_3x_1 \\
&= x_1^3 + x_2^3 + x_3^3 + 3(x_1(x_2x_1 + x_3x_1 + x_2x_3) + x_2(x_2x_1 + x_3x_1 + x_2x_3) + \\
&+ x_3(x_2x_1 + x_3x_1 + x_2x_3)) - 3x_2x_3x_1 \\
&= x_1^3 + x_2^3 + x_3^3 + 3(x_1 + x_2 + x_3)(x_2x_1 + x_3x_1 + x_2x_3) - 3x_2x_3x_1 \\
&= x_1^3 + x_2^3 + x_3^3 + 3(e_1)(e_2) - 3e_3
\end{aligned}
$$

Por lo tanto, al despejar,

$$x_1^3 + x_2^3 + x_3^3 = e_1^3 + 3e_3 - 3e_1e_2$$

□

Problema 8 (Problema 12)**.** *If $p(x) = x^n - 1$ prove that the Galois group of $p(x)$ over the field of rational numbers is abelian.*

Solución. Si F es un campo que contiene todas las raíces $n-$ésimas de la unidad, $n \in \mathbb{Z}^+, 1 \in F - \{0\}, K$ el campo de descomposición de $x^n - 1 \in F[x]$, entonces por la parte (ii) del **lema 5.12** usando $a = 1$, el grupo de Galois de $p(x)$ sobre $\mathbb{Q}$ es abeliano. □