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
30 de octubre de 2022

Tarea 22

Problemas 2, 5, 6, 7, 11, 12 y 13, sección 5.3

Problema 1 (Problema 2). *In the proof of Theorem 5.3.1, prove in all detail that the elements $1+V, x+V, \ldots, x^{n-1}+V$ form a basis of E over F.*

Demostración. **Detalles del teorema demostrado en clase:**

> **Teorema 48** (5G). *Si F es un campo, $p(x) \in F[x], gr(p) \geq 1$, irreducible sobre F, entonces existe E, extensión de F tal que $[E:F] = gr(p)$ y E contiene por lo menos una raíz de $p(x)$.*
>
> ***Demostración.*** Por el lema 3.22, $((p(x)))$ es un ideal maximal de F en $F[x] \implies$ por el teorema 3B, $F[x]/((p))$ es un campo. Si $f(x)+[p(x)] \in F[x]/(p(x))$ con $f(x) \in F[x]$, aplicando el algoritmo de la división en $F[x]$ (lema 3.17), a $f(x)$ y $p(x), \exists q(x), r(x) \in F[x], r(x) = 0$ o $r(x) = \sum_{i=0}^{gr(p)-1} \alpha_i x^i$, i.e. $g(r) < gr(p) \implies f(x)+[p(x)] = (q(x)p(x)+r(x))+[p(x)] = [q(x)p(x)+[p(x)]]+[r(x)+[p(x)]] = [0+[p(x)]]+[r(x)+[p(x)]] = [p(x)]+[r(x)+[p(x)]] = r(x)+[p(x)] = \sum_{i=0}^{gr(p)-1} \alpha_i x^i + [p(x)] = \sum_{i=0}^{gr(p)-1}(\alpha_i + [p(x)]) = \sum_{i=0}^{gr(p)-1} \alpha_i (x^i + [p(x)]) = \sum_{i=0}^{gr(p)-1} \alpha_i (x+(p(x)))^i \implies F[x]/(p(x)) = \langle \{1, \cdots, (x+[p(x)])^{gr(p)-1}\} \rangle_F$ Sea $\phi : F[x] \to F[x]/(p(x))$. Si $\beta_0, \cdots, \beta_{gr(p)-1} \in F \ni ((p(x))) = \sum_{i=0}^{gr(p)-1} \beta_i (x+[p(x)])^i = \left(\sum_{i=0}^{gr(p)-1} \beta_i x^i\right) + [p(x)]$. Sea $g(x) = \sum_{i=0}^{gr(p)-1} \beta_i x^i \in F[x] \implies [p(x)] = g(x)+[p(x)] \implies g(x) \in [p(x)] \implies p(x)|g(x) \implies gr(p)-1 \geq gr(q) \geq gr(p) \implies p(x) = 0 \implies \beta_0 = \cdots = \beta_{gr(p)-1} \implies \{1, \cdots, (x+[p(x)])^{gr(p)-1}\}$ es linealmente independiente es $F[x]/(p(x))$ sobre $F \implies \{1, \cdots, (x+[p(x)])^{gr(p)-1}\}$ es una base de $F[x]/(p(x))$ sobre F. Nótese que además, $p(x+[p(x)]) =$

∎

Problema 2 (Problema 5)**.** *In Example 3 at the end of this section prove that $F(\omega)$ is the splitting field of $x^4 + x^2 + 1$.*

Demostración. Nótese que

$$f(x) = x^4 + x^2 + 1 = (x - w)(x + w)(x - w^2)(x + w^2),$$

tal que $f(x)$ es irreducible sobre F en $F(w)$. ■

Problema 3 (Problema 6)**.** *Let F be the field of rational numbers. Determine the degrees of the splitting fields of the following polynomials over F.*

1. $x^4 + 1$.

   Demostración. Sea

   $$f(x) = x^4 + 1 = (x - w)(x + w)(x - w^3)(x + w^3),$$

   en donde las raíces son complejas. Entonces $x^4 + 1$ es irreducible por criterio de Eisenstein. Además su grado es 4. ■

2. $x^6 + 1$.

   Demostración. Sea

   $$f(x) = x^6+1 = (x-i)(x+i)(x^4+x^2+1) = (x-i)(x+i)(x-w)(x+w)(x-w^2)(x+w^2),$$

   entonces $f(x)$ es irreducible sobre $F(w)$. Además por el **Problema 2**, sabíamos que $^4 + x^2 + 1$ es irreducible sobre F con grado 4 por Eisenstein. Por lo tanto, $x^6 + 1$ también es de grado 4. ■

3. $x^4 - 2$.

   Demostración. Sea

   $$f(x) = x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2}),$$

   de esto tenemos que el campo de descomposición es $F(\sqrt[4]{2}, i)$. Además, nótese que $x^2 + 1$ es irreducible en $F(\sqrt[4]{2})$ tal que $[F(\sqrt[4]{2}, i) : F(\sqrt[4]{2})] = 2$ y por otra parte, se tiene que $[F(\sqrt[4]{2}) : F] = 4$. Entonces, el grado es $[F(\sqrt[4]{2}, i) : F(\sqrt[4]{2})[F(\sqrt[4]{2}) : F]] = 8$. ■

4. $x^5 - 1$.

   Demostración. Sea

   $$f(x) = x^5 - 1 = (x - w)(x - w^2)(x - w^3)(x - w^4)(x - w^5),$$

   entonces $f(x)$ es irreducible sobre $F(w)$. Por otra parte, nótese que $x^4+x^3+x^2+x+1$ es irreducible en F con grado 4, y por lo tanto $x^5 - 1$ también tiene grado 4. ■

5. $x^6 + x^3 + 1$.

Demostración. Sea

$$f(x) = x^6 + x^3 + 1 = (x - w)(x + w)(x - w^4)(x + w^4)(x - w^7)(x + w^7),$$

entonces $f(x)$ es irreducible sobre $F(w)$. Entonces, por Eisenstein el grado es 6. ■

Problema 4 (Problema 7)**.** *If p is a prime number, prove that the splitting field over F, the field of rational numbers, of the polynomial $x^p - 1$ is of degree $p - 1$.*

Demostración. Sea

$$f(x) = x^p - 1 = (x - 1)(x - w)(x - w^2) \cdots (x - w^{p-1}),$$

entonces $F(w)$ es el campo de descomposición de $f(x)$ sobre F. Ahora, proponemos una función $g(x)$ que es irreducible sobre los irracionales definida como $g(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, tal que $g(w) = 0$. Entonces el grado del polinomio $f(x)$ es $[F(w) : F] = p - 1$. ■

Problema 5 (Problema 11)**.** *If E is an extension of F and if $f(x) \in F[x]$ and if ϕ is an automorphism of E leaving every element of F fixed, prove that ϕ must take a root of $f(x)$ lying in E into a root of $f(x)$ in E.*

Demostración. Sea

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + a_n x^n \in F[x],$$

ahora bien, sea w una raíz de $f(x)$, tal que:

$$f(w) = a_0 + a_1 w + \cdots + a_{n-1} w^{n-1} + a_n w^n = 0,$$

ahora considerando el automorfismo ϕ, se tiene,

$$\begin{aligned} 0 &= \phi(f(w)) \\ &= \phi\left(a_0 + a_1 w + \cdots + a_{n-1} w^{n-1} + a_n w^n\right) \\ &= a_0 + a_1 \phi(w) + \cdots + a_{n-1}(\phi(w))^{n-1} + a_n(\phi(b))^n \end{aligned}$$

Por lo tanto, $\phi(w)$ es una raíz también de $f(x)$ en E. ■

Problema 6 (Problema 12)**.** *Prove that $F(\sqrt[3]{2})$, where F is the field of rational numbers, has no automorphisms other than the identity automorphism.*

Demostración. Sea ϕ un automorfismo de $\mathbb{Q}(\sqrt[3]{2})$, ya que $\phi(1) = 1$ entonces:

$$\phi\left(\frac{p}{q}\right) = \frac{p\phi(1)}{q\phi(1)} = \frac{p}{q}, \forall p, q \in \mathbb{Z}$$

Port otra parte, nótese que

$$\phi(\sqrt[3]{2}) = \phi((\sqrt[3]{3})^3) = \phi(2) = 2,$$

es decir que $\phi(\sqrt[3]{2})$ es un subcampo de $\mathbb{R}$ y además tenemos que $\sqrt[3]{2}$ es la única raíz de $x^3 - 2$ en $\mathbb{Q}$, entonces $\phi(\sqrt[3]{2}) = \sqrt[3]{2}$. Ahora bien, nótese que los elementos de $\mathbb{Q}(\sqrt[3]{2})$ son de la forma $a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2$, entonces considérese:

$$\begin{aligned} \phi\left(a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2\right) &= \phi(a_0) + \phi(a_1)\phi(\sqrt[3]{2}) + \phi(a_2)\phi((\sqrt[3]{2})^2) \\ &= a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2 \end{aligned}$$

Entonces, tenemos que $\phi(a_0) = a_0, \phi(a_1) = a_1$ y $\phi(a_2) = a_2$. Por lo tanto, $\phi = I_{\mathbb{Q}(\sqrt[3]{2})}$. ■

Problema 7 (Problema 13)**.** *Using the result of Problem 11, prove that if the complex number α is a root of the polynomial $p(x)$ having real coefficients then $\bar{\alpha}$, the complex conjugate of α, is also a root of $p(x)$.*

Demostración. Sea ϕ un automorfismo de los complejos a los complejos, definido como

$$\phi(z) = \overline{z},$$

por el **Problema 11**, si α es un raíz de $p(x)$, entonces $\phi(\alpha) = \overline{\alpha}$ es también una raíz de $p(x)$. ■