Sección 30

En los Ejercicios del 4 al 9, da una base para el espacio vectorial indicado sobre el campo:

4. $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$

   Solución: Como $\sqrt{2}$ es una raíz del irreducible $x^2 - 2$ de grado 2, el Teorema 30.23 muestra que una base es $\{1, \sqrt{2}\}$.

5. $\mathbb{R}(\sqrt{2})$ sobre $\mathbb{R}$

   Solución: Dado que $\sqrt{2}$ está en $\mathbb{R}$ y es una raíz del polinomio $x - \sqrt{2}$ de grado 1, el Teorema 30.23 muestra que una base es $\{1\}$.

6. $\mathbb{Q}(\sqrt[3]{2})$ sobre $\mathbb{Q}$

   Solución: Como $\sqrt[3]{2}$ es una raíz del irreducible $x^3 - 2$ de grado 3, según el Teorema 30.23 una base es $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$.

7. $\mathbb{C}$ sobre $\mathbb{R}$

   Solución: Dado que $\mathbb{C} = \mathbb{R}(i)$ donde i es una raíz del irreducible x^2+1 de grado 2, el Teorema 30.23 muestra que una base es $\{1, i\}$.

8. $\mathbb{Q}(i)$ sobre $\mathbb{Q}$

   Solución: Dado que i es una raíz del irreducible $x^2 + 1$ de grado 2, el Teorema 30.23 muestra que una base es $\{1, i\}$.

9. $\mathbb{Q}(\sqrt[4]{2})$ sobre $\mathbb{Q}$

   Solución: Dado que $\sqrt[4]{2}$ es una raíz del irreducible $x^4 - 2$ de grado 4, según el Teorema 30.23 una base es $\{1, \sqrt[4]{2}, \sqrt{2}, (\sqrt[4]{2})^3\}$.

Sección 31

Calculos

En los Ejercicios 1 a 13, encuentra el grado y una base para la extensión de campo dada. Prepárate para justificar tus respuestas.

1. $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$

   Solución: Como $\sqrt{2}$ es una raíz del irreducible $x^2 - 2$, el grado es 2 y una base es $\{1, \sqrt{2}\}$.

2. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}$

   Solución: Por el Ejemplo 31.9, el grado es 4 y una base es $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.

3. $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{8})$ sobre $\mathbb{Q}$

   Solución: Observamos que $\sqrt{18} = \sqrt{2} \cdot \sqrt{3}\sqrt{3}$. Por lo tanto, $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{18})$ y $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ son el mismo campo. El grado es 4 y una base es $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ según el Ejemplo 31.9.

4. $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$ sobre $\mathbb{Q}$

   Solución: Dado que $\sqrt{3} \notin \mathbb{Q}(\sqrt[3]{2})$ porque $\mathbb{Q}(\sqrt{3})$ tiene grado 2 sobre $\mathbb{Q}$ mientras que $\mathbb{Q}(\sqrt[3]{2})$ tiene grado 3, y 2 no divide a 3, el grado de $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$ sobre $\mathbb{Q}$ es 6. Formamos productos a partir de las bases $\{1, \sqrt{3}\}$ para $\mathbb{Q}(\sqrt{3})$ sobre $\mathbb{Q}$ y $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$ para $\mathbb{Q}(\sqrt[3]{2})$ sobre $\mathbb{Q}(\sqrt{3})$, obteniendo $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \sqrt{3}, \sqrt{3}\sqrt[3]{2}, \sqrt{3}(\sqrt[3]{2})^2\}$ como una base.

5. $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ sobre $\mathbb{Q}$

   Solución: Como en la solución al Ejercicio 4, la extensión tiene grado 6. Tomando productos de las bases $\{1, \sqrt{2}\}$ para $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$ y $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$ para $\mathbb{Q}(\sqrt[3]{2})$ sobre $\mathbb{Q}(\sqrt{2})$, vemos que $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \sqrt{2}, \sqrt{2}\sqrt[3]{2}, \sqrt{2}(\sqrt[3]{2})^2\}$ es una base. Es fácil ver que $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$ ya que $2^{1/6} = (2^{1/3})^{1/2}$, así que otra base es $\{1, 2^{1/6}, (2^{1/6})^2, (2^{1/6})^3, (2^{1/6})^4, (2^{1/6})^5\}$.

6. $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ sobre $\mathbb{Q}$

   Solución: Como se muestra en el Ejemplo 31.9, tenemos grado 4, entonces $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ y una base es $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ tal como en el Ejemplo 31.9.

7. $\mathbb{Q}(\sqrt{2}\sqrt{3})$ sobre $\mathbb{Q}$

   Solución: Porque $\sqrt{2}\sqrt{3} = \sqrt{6}$, vemos que el campo es $\mathbb{Q}(\sqrt{6})$ que tiene grado 2 sobre $\mathbb{Q}$ y una base es $\{1, \sqrt{6}\}$.

8. $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$ sobre $\mathbb{Q}$

   Solución: Como en la solución al Ejercicio 4, vemos que la extensión es de grado 6. Formamos productos de las bases $\{1, \sqrt{2}\}$ para $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$ y $\{1, \sqrt[3]{5}, (\sqrt[3]{5})^2\}$ para $\mathbb{Q}(\sqrt[3]{5})$ sobre $\mathbb{Q}(\sqrt{2})$, obteniendo $\{1, \sqrt[3]{5}, (\sqrt[3]{5})^2, \sqrt{2}, \sqrt{2}\sqrt[3]{5}, \sqrt{2}(\sqrt[3]{5})^2\}$ como una base.

9. $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{6}, \sqrt[3]{24})$ sobre $\mathbb{Q}$

   Solución: Ahora, $\frac{\sqrt[3]{6}}{\sqrt[3]{2}} = \sqrt[3]{3}$ y $\sqrt[3]{24} = 2\sqrt[3]{3}$, entonces $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{6}, \sqrt[3]{24}) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})$. El grado sobre $\mathbb{Q}$ es 9, y tomamos productos de las bases $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$ y $\{1, \sqrt[3]{3}, (\sqrt[3]{3})^2\}$ para $\mathbb{Q}(\sqrt[3]{2})$ sobre $\mathbb{Q}$ y $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})$ sobre $\mathbb{Q}(\sqrt[3]{2})$ respectivamente, obteniendo la base $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \sqrt[3]{3}, \sqrt[3]{6}, \sqrt[3]{12}, \sqrt[3]{9}, \sqrt[3]{1$

10. $\mathbb{Q}(\sqrt{2}, \sqrt{6})$ sobre $\mathbb{Q}(\sqrt{3})$

    Solución: Dado que $\mathbb{Q}(\sqrt{2}, \sqrt{6}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, la extensión tiene grado 2 sobre $\mathbb{Q}(\sqrt{3})$ y tomamos el conjunto $\{1, \sqrt{2}\}$ como una base.

11. $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ sobre $\mathbb{Q}(\sqrt{3})$

    Solución: Por el Ejemplo 31.9, $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, entonces el grado de la extensión es 2 y tomamos el conjunto $\{1, \sqrt{2}\}$ como una base sobre $\mathbb{Q}(\sqrt{3})$.

12. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}(\sqrt{2} + \sqrt{3})$

    Solución: Por el Ejemplo 31.9, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, entonces el grado de la extensión es 1 y tomamos el conjunto $\{1\}$ como una base sobre $\mathbb{Q}(\sqrt{2} + \sqrt{3})$.

13. $\mathbb{Q}(\sqrt{2}, \sqrt{6} + \sqrt{10})$ sobre $\mathbb{Q}(\sqrt{3} + \sqrt{5})$

    Solución: Ahora, $\sqrt{6} + \sqrt{10} = \sqrt{2}(\sqrt{3} + \sqrt{5})$, entonces $\mathbb{Q}(\sqrt{2}, \sqrt{6} + \sqrt{10}) = \mathbb{Q}(\sqrt{2}, \sqrt{3} + \sqrt{5})$. El grado de la extensión es 2 y una base sobre $\mathbb{Q}(\sqrt{3} + \sqrt{5})$ es $\{1, \sqrt{2}\}$.

Teoría

22. Demuestra que si $(a + bi)$ pertenece a $\mathbb{C}$ donde a, b pertenecen a $\mathbb{R}$ y $b \neq 0$, entonces $\mathbb{C} = \mathbb{R}(a + bi)$.

    Solución:

    Si $b \neq 0$, entonces $a+bi$ es un número complejo donde a, b son números reales. Por el Teorema 31.3, $a + bi$ es algebraico sobre $\mathbb{R}$. Luego, por el Teorema 31.4,

    $$[\mathbb{C} : \mathbb{R}] = [\mathbb{C} : \mathbb{R}(a + bi)][\mathbb{R}(a + bi) : \mathbb{R}] = 2.$$

    Dado que $a + bi \notin \mathbb{R}$, debemos tener $[\mathbb{R}(a + bi) : \mathbb{R}] = 2$, por lo tanto $[\mathbb{C} : \mathbb{R}(a + bi)] = 1$. Así, $\mathbb{C} = \mathbb{R}(a + bi)$.

23. Muestra que si E es una extensión finita de un campo F y $[E : F]$ es un número primo, entonces E es una extensión simple de F y, de hecho, $E = F(a)$ para cada a en E que no está en F.

    Solución:

    Sea α cualquier elemento en E que no esté en F. Entonces, $[E : F] = [E : F(\alpha)][F(\alpha) : F] = p$ para algún primo p según el Teorema 31.4. Dado que α no está en F, sabemos que $[F(\alpha) : F] > 1$, por lo que debemos tener $[F(\alpha) : F] = p$ y, por lo tanto, $[E : F(\alpha)] = 1$. Esto muestra que $E = F(\alpha)$, que es lo que deseamos demostrar.

24. Demuestra que $x^3 - 3$ es irreducible sobre $\mathbb{Q}(\sqrt[3]{2})$.

    Solución:

    Si $x^2 - 3$ fuera reducible sobre $\mathbb{Q}(\sqrt[3]{2})$, entonces se factorizaría en factores lineales sobre $\mathbb{Q}(\sqrt[3]{2})$, por lo que $\sqrt{3}$ estaría en el campo $\mathbb{Q}(\sqrt[3]{2})$, y tendríamos $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt[3]{2})$. Pero entonces, por el Teorema 31.4,

    $$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}].$$

    Esta ecuación es imposible porque $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ mientras que $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$.

26. Sea E una extensión de campo finita de F. Sea D un dominio integral tal que $F \subseteq D \subseteq E$. Demuestra que D es un campo.

    Solución:

    Solo necesitamos demostrar que para cada $\alpha \in D$ con $\alpha \neq 0$, su inverso multiplicativo $1/\alpha$ también está en D. Como E es una extensión finita de F, sabemos que α es algebraico sobre F. Si $\deg(\alpha, F) = n$, entonces por el Teorema 30.23, tenemos:

    $$F(\alpha) = \left\{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in F \text{ para } i = 0, \ldots, n-1\right\}.$$

    En particular, $1/\alpha \in F(\alpha)$, por lo que $1/\alpha$ es un polinomio en α con coeficientes en F, y por lo tanto está en D.

27. Demuestra en detalle que $\mathbb{Q}(\sqrt{3} + \sqrt{7}) = \mathbb{Q}(\sqrt{3}, \sqrt{7})$.

    Solución:

Es obvio que $\mathbb{Q}(\sqrt{3}+\sqrt{7}) \subseteq \mathbb{Q}(\sqrt{3},\sqrt{7})$. Ahora, $(\sqrt{3}+\sqrt{7})^2 = 10+2\sqrt{21}$, por lo que $\sqrt{21} \in \mathbb{Q}(\sqrt{3}+\sqrt{7})$. Por lo tanto,

$$(\sqrt{3}+\sqrt{7}) - \sqrt{7} = \sqrt{3}$$

también está en $\mathbb{Q}(\sqrt{3}+\sqrt{7})$. De manera similar, $\sqrt{3}+\sqrt{7}-\sqrt{3} = \sqrt{7}$, por lo que $\mathbb{Q}(\sqrt{3},\sqrt{7}) \subseteq \mathbb{Q}(\sqrt{3}+\sqrt{7})$. Por lo tanto, $\mathbb{Q}(\sqrt{3},\sqrt{7}) = \mathbb{Q}(\sqrt{3}+\sqrt{7})$.

28. Generalizando el Ejercicio 27, demuestra que si $\sqrt{a}+\sqrt{b} \neq 0$, entonces $\mathbb{Q}(\sqrt{a}+\sqrt{b}) = \mathbb{Q}(\sqrt{a},\sqrt{b})$ para todo a y b en $\mathbb{Q}$. [Pista: Calcula $\frac{a-b}{\sqrt{a}+\sqrt{b}}$.]

    Solución:

    Si $a = b$, el resultado es claro; asumimos entonces que $a \neq b$. Es evidente que $\mathbb{Q}(\sqrt{a}+\sqrt{b}) \subseteq \mathbb{Q}(\sqrt{a},\sqrt{b})$. Ahora mostraremos que $\mathbb{Q}(\sqrt{a},\sqrt{b}) \subseteq \mathbb{Q}(\sqrt{a}+\sqrt{b})$. Sea $\alpha = \frac{a-b}{\sqrt{a}+\sqrt{b}} \in \mathbb{Q}(\sqrt{a}+\sqrt{b})$. Entonces $\alpha = \sqrt{a}-\sqrt{b}$. Por lo tanto, $\mathbb{Q}(\sqrt{a}+\sqrt{b})$ contiene $\frac{1}{2}[\alpha+(\sqrt{a}+\sqrt{b})] = \frac{1}{2}(2\sqrt{a}) = \sqrt{a}$ y por lo tanto también contiene $(\sqrt{a}+\sqrt{b})-\sqrt{a} = \sqrt{b}$. Así que $\mathbb{Q}(\sqrt{a},\sqrt{b}) \subseteq \mathbb{Q}(\sqrt{a}+\sqrt{b})$.

29. Sea E una extensión finita de un campo F, y sea $p(x)$ en $F[x]$ irreducible sobre F y tenga grado que no sea un divisor de $[E:F]$. Demuestra que $p(x)$ no tiene ceros en E.

    Solución:

    Si un cero α de $p(x)$ estuviera en E, entonces como $p(x)$ es irreducible sobre F, tendríamos $[F(\alpha):F] = \deg(p(x))$, y $[F(\alpha):F]$ sería un divisor de $[E:F]$ por el Teorema 31.4. Pero por hipótesis, esto no es el caso. Por lo tanto, $p(x)$ no tiene ceros en E.

30. Sea E una extensión de campo de F. Sea a en E algebraico de grado impar sobre F. Demuestra que a^2 es algebraico de grado impar sobre F, y $F(a) = F(a^2)$.

    Solución:

    Como $F(a)$ es una extensión finita de F y $a^2 \in F(a)$, el Teorema 31.3 muestra que a^2 es algebraico sobre F. Si $F(a^2) \neq F(a)$, entonces $F(a)$ sería una extensión de $F(a^2)$ de grado 2, porque a es una raíz de x^2-a^2. Por el Teorema 31.4, esto significaría que 2 divide el grado de $F(a)$ sobre F, lo cual es imposible ya que el grado de a es impar. Por lo tanto, $F(a) = F(a^2)$.

31. Demuestra que si F, E y K son campos con $F \leq E \leq K$, entonces K es algebraico sobre F si y solo si E es algebraico sobre F, y K es algebraico sobre E. (No debes asumir que las extensiones son finitas.)

    Solución:

    Supongamos que K es algebraico sobre F. Entonces cada elemento de K es una raíz de un polinomio no nulo en $F[x]$, y por lo tanto en $E[x]$. Esto muestra que K es algebraico sobre E. Por supuesto, E es algebraico sobre F, porque cada elemento de E también es un elemento de K.

    Recíprocamente, supongamos que K es algebraico sobre E y que E es algebraico sobre F. Sea $\alpha \in K$. Debemos mostrar que α es algebraico sobre F. Como K es algebraico sobre E, α es una raíz de un polinomio no nulo en $E[x]$. Porque E es algebraico sobre F, los coeficientes de este polinomio son algebraicos sobre F. Por lo tanto, α es algebraico sobre F, y K es algebraico sobre F.

32. Sea E una extensión de campo de un campo F. Demuestra que todo a en E que no está en el cierre algebraico $\overline{F}_E$ de F en E es trascendente sobre $\overline{F}_E$.

    Solución:

    Si α es algebraico sobre $\overline{F}_E$, entonces $F(\alpha)$ es una extensión finita de F, y por lo tanto, α es algebraico sobre F. Pero entonces α está en el cierre algebraico de F en E, lo cual es una contradicción. Por lo tanto, α es trascendente sobre $\overline{F}_E$.

34. Demuestra que si E es una extensión algebraica de un campo F y contiene todos los ceros en $\overline{F}$ de cada $f(x)$ en $F[x]$, entonces E es un campo algebraicamente cerrado.

    Solución:

    Sea $\alpha \in E$ y sea $p(x) = \text{irr}(\alpha, F)$ de grado n. Ahora, $p(x)$ se factoriza en $(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ en $F[x]$. Debido a que por hipótesis todos los ceros de $p(x)$ en F también están en E, vemos que esta misma factorización también es válida en $E[x]$. Por lo tanto,

    $$p(\alpha) = (\alpha - \alpha_1)(\alpha - \alpha_2) \cdots (\alpha - \alpha_n) = 0,$$

    entonces $\alpha = \alpha_i$ para algún i. Esto muestra que $F \leq E \leq \overline{F}$. Debido a que, por definición, F contiene solo elementos que son algebraicos sobre F y E contiene todos estos, vemos que $E = \overline{F}$ y, por lo tanto, es algebraicamente cerrado.

35. Demuestra que ningún campo finito de característica impar es algebraicamente cerrado. (De hecho, tampoco ningún campo finito de característica 2 es algebraicamente cerrado.) [Pista: Mediante un conteo, demuestra que para tal campo finito F, algún polinomio $x^2 - a$, para algún $a \in F$, no tiene cero en F. Consulta el Ejercicio 32, Sección 29.]

    Solución:

    Si F es un campo finito de característica impar, entonces $1 \neq -1$ en F. Debido a que $1^2 = (-1)^2 = 1$, los cuadrados de los elementos de F pueden recorrer a lo sumo $|F| - 1$ elementos de F, por lo que hay algún $a \in F$ que no es un cuadrado. El polinomio $x^2 - a$ entonces no tiene ceros en F, por lo que F no es algebraicamente cerrado.