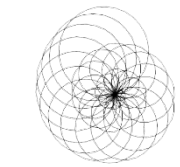

Universidad Nacional Autónoma de México
Facultad de Ciencias

Algebra Moderna II

Examen 3

Por: Lorenzo Antonio Alvarado Cabrera

Problema 1. –

Definición. Sea F un campo, $E_1, E_2 \subseteq F$ subcampos de F, la composición de E_1 y E_2 denotada por $E_1 \vee E_2$ es

$$E_1 \vee E_2 = \bigcap \{K \subseteq F : E_1 \cup E_2 \subseteq K \text{ y } K \text{ es subcampo de } F\}$$

1. (3 puntos) Sea F un campo, $E, E_1, \ldots, E_n$ subcampos de F.

   a) Demuestra que
   $$E_1 \cap \ldots \cap E_n$$
   Es el $\subseteq$-mayor campo contenido en E_i para $i \in \{1, \ldots, n\}$. [1]

   b) Demuestra que
   $$E_1 \vee \ldots \vee E_n$$
   Es el $\subseteq$-menor campo que contiene a E_i para $i \in \{1, \ldots, n\}$. [2]

   c) Sea $E \subseteq F$ un subcampos, y $\alpha_1, \ldots, \alpha_n \in F$. Entonces
   $$F(\alpha_1) \vee \ldots \vee F(\alpha_n) = F(\alpha_1, \ldots, \alpha_n)$$

Demostración:

(*a*) Sea $i \in \{1,...,n\}$ fijo. Veamos que $E = E_1 \cap \ldots \cap E_n$ es subcampo de F.

- De forma clara $E \subseteq E_i \subseteq F$ para cada $i \in \{1,...,n\}$.
- Como cada E_j es subcampo de F entonces $0_F \in E_j$ para cada j por lo que $0_F \in E$.
- Sean $a, b \in E$ entonces $a, b \in E_j \ \forall j$, y al ser cada uno subcampo tendremos que $a - b \in E_j \ \forall j$ por lo que $a - b \in E$.
- Sean $a, b \in E$ con $b \neq 0$, entonces $a, b \in E_j \ \forall j$, y al ser cada uno subcampo tendremos que $ab^{-1} \in E_j \ \forall j$ por lo que $ab^{-1} \in E$.

Por tanto, es subcampo de F.

Ahora veamos que es el menor subcampo que contiene a los E_i´s (en términos de contención). Sea K subcampo de F tal que $K \subseteq E_i$ para cada $i \in \{1,...,n\}$, entonces $\bigcap_{i=1}^{n} K \subseteq \bigcap_{i=1}^{n} E_i = E$, es decir, $K \subseteq E$, por lo que E es el mayor subcampo contenido todos los E_i´s.

(*b*) Llamemos $A_n = \bigcap\{K \subseteq F : E_1 \cup .... \cup E_n \subseteq K \text{ y } K \text{ subcampo de } F\} = \bigcap_{K \in B_n} K$, donde $B_n = \{K \subseteq F : E_1 \cup .... \cup E_n \subseteq K \text{ y } K \text{ subcampo de } F\}$. Con esto es claro que como para cada $K \in B_n$, $E_i \subseteq E_1 \cup .... \cup E_n \subseteq K$ entonces $E_i \subseteq \bigcap_{K \in B_n} K = A_n$ para cada i.

Veamos que A_n es subcampo de F. En efecto:

- Tenemos que $\forall K \in B_n$, $K \subseteq F$ entonces $A_n = \bigcap_{K \in B_n} K \subseteq F$.
- Sabemos que $\forall K \in B_n$, K es subcampo de F por lo que $0_F \in K$, $\forall K \in B_n$, entonces $0_F \in \bigcap_{K \in B_n} K = A_n$.
- Sean $a, b \in A_n$ entonces $a, b \in K \ \forall K \in B_n$, y al ser cada uno subcampo tendremos que $a - b \in K \ \forall K \in B_n$ por lo que $a - b \in A_n$.
- Sean $a, b \in A_n$ con $b \neq 0$, entonces $a, b \in K \ \forall K \in B_n$, y al ser cada uno subcampo tendremos que $ab^{-1} \in K \ \forall K \in B_n$ por lo que $ab^{-1} \in A_n$.

Por tanto, es subcampo de F.

Ahora veamos que es el menor subcampo que contiene a los E_i´s (en términos de contención). Sea L subcampo de F tal que $E_i \subseteq L$ para cada $i \in \{1,...,n\}$, entonces $E_1 \cup ... \cup E_n \subseteq L$ por lo que $L \in B_n$, entonces $A_n = \bigcap_{K \in B_n} K \subseteq L$, es decir $A_n \subseteq L$.

Con esto último igualmente demostramos por la definición de la composición que $E_1 \vee \cdots \vee E_n = A_n$ (ya que esta era el menor subcampo que contenía a los conjuntos). Y por todo lo anterior tenemos que es subcampo de F.

(*c*) En efecto, por definición

$$E(\alpha_1,...,\alpha_n) = E(S) \coloneqq \bigcap_{E' \in \pounds} E'$$

donde $S = \{\alpha_1,...,\alpha_n\}$ y $\pounds = \{E' \subseteq F : E \cup S \subseteq E' \text{ y } E' \text{ subcampo de } F\}$, es decir, es el menor subcampo de F que contiene a E y a cada α_i.

PD $E(\alpha_1) \vee \cdots \vee E(\alpha_n)$ cumple dicha definición.

Por el inciso anterior sabemos que como cada $E(\alpha_i)$ es subcampo de F, entonces $E(\alpha_1)\vee\cdots\vee E(\alpha_n)$ es subcampo de F. Por otro lado tenemos por el inciso anterior sabemos que $E(\alpha_1)\vee\cdots\vee E(\alpha_n)$ es el menor subcampo que contiene a cada $E(\alpha_i)$ y por la definición de $E(\alpha_i)$ es el menor subcampo que contiene a E y a α_i, por tanto, $E(\alpha_1)\vee\cdots\vee E(\alpha_n)$ contiene a E y a cada α_i. Finalmente veamos que es el menor, sea L subcampo de F tal que contiene a E y a cada α_i, entonces en particular contiene a α_j para $j=1,...,n$ por lo que por definición $E(\alpha_j)\subseteq L$, y nuevamente por el inciso anterior como $E(\alpha_j)\subseteq L$ para cada j, entonces $E(\alpha_1)\vee\cdots\vee E(\alpha_n)\subseteq L$. Con todo lo anterior $E(\alpha_1)\vee\cdots\vee E(\alpha_n)=E(\alpha_1,...,\alpha_n)$.

■

Problema 2. –

a) Sea F un campo, y K/F una extensión de campo tal que K es algebraicamente cerrado. Sea

$$\bar{F}=\{a\in K : a \textit{ es algebráico sobre } F\}.$$

Entonces $\bar{F}$ es una cerradura algebráica de F.

b) Considera **el conjunto de los números algebráicos**:

$$\mathbb{A}=\{a\in\mathbb{C} : a \textit{ es algebráico sobre } \mathbb{Q}\}$$

Demuestra que $\mathbb{A}/\mathbb{Q}$ es una extensión algebráica no finita.

Demostración:

(a) Tenemos que ver 3 cosas; $\overline{F}$ es campo, $\overline{F}$ es extensión algebraica de F y todo polinomio $f(x)\in F[x]$ se factoriza linealmente en $\overline{F}$.

⊙ Tenemos que $\overline{F}$ es subcampo.

• De forma clara $\overline{F}\subseteq K$.

• Tenemos que $f(x)=x\in F[x]$ es tal que $f(0)=0$, siendo un polinomio monico que se anula en 0 por lo que $0\in\overline{F}$.

• Ahora, debemos demostrar que si $a,b\in\overline{F}$ entonces $a+b, ab^{-1}\in\overline{F}$, esto es queremos demostrar que $a+b$ y ab^{-1} son algebraicos sobre F, pero recordemos la proposición 3.3.4 que nos dice que si tenemos una extensión finita, entonces esta es algebraica, es decir, todo elemento de la extensión será algebraico sobre el campo extendido. Con esto en mano consideremos la extensión de campos $F(a,b)/F$ y bastara con probar que es una extensión finita, pues de hacerlo, será una extensión algebraica y como $a,b\in F(a,b)$ y $F(a,b)$ es campo entonces $a+b, ab^{-1}\in F(a,b)$ serán algebraicos sobre F. Vayamos a ello.

Como $b \in \overline{F}$, entonces existe un polinomio $p_b(x) \in F[x]$ monico e irreducible tal que $p_b(b) = 0$ (teorema 3.3.6) y además $[F(b) : F] = \text{grad}(p_b(x)) < \infty$. Igualmente como $a \in \overline{F}$, entonces existe un polinomio $p_a(x) \in F[x]$ monico e irreducible tal que $p_a(a) = 0$ y además $[F(a) : F] = \text{grad}(p_a(x)) < \infty$. Entonces por la proposición 3.3.11 $[F(a,b) : F] \leq [F(a) : F][F(b) : F] < \infty$, por tanto $[F(a,b) : F]$ es una extensión algebraica, y entonces $a + b, ab^{-1} \in \overline{F}$.

⊙ $\overline{F}$ es extensión algebraica.
Esto es claro, pues si $a \in F \Rightarrow a$ es algebraico sobre F ya que $f(x) = x - a$ es un polinomio monico que se anula en a, por lo que $F \subseteq \overline{F}$ entonces $\overline{F} / F$ es una extensión. Mas aun, si $a \in \overline{F}$ entonces por definición del conjunto a es algebraico sobre F por lo que $\overline{F} / F$ es extensión algebraica.

⊙ Todo polinomio $f(x) \in F[x]$ se factoriza linealmente en $\overline{F}$.
En efecto, sea $f(x) \in F[x]$ con $grad(f) = n$, entonces todas las raíces de f están en $\overline{F}$, pues si suponemos que existe $\beta \in K - \overline{F}$ tal que $f(\beta) = 0$, pues necesariamente por la definición de $\overline{F}$, $\beta \in \overline{F}$!!! y llegamos a un absurdo, pues β esta y no esta en $\overline{F}$. Por tanto $\beta \in \overline{F}$.
Con esto tenemos que todas las raíces de $f(x)$ están en $\overline{F}$, sean $\alpha_1, .., \alpha_n \in \overline{F}$ dichas raíces distintas, entonces por el corolario 3.2.10 $x - \alpha_1 \mid f(x) \Rightarrow f(x) = f_1(x)(x - \alpha_1)$ y como $grad(f) = n$ entonces $grad(f_1) = n - 1$, de igual forma $x - \alpha_2 \mid f(x) \Rightarrow x - \alpha_2 \mid f_1(x)(x - \alpha_1)$ y como $x - \alpha_2 \nmid x - \alpha_1$ entonces $f_1(x) = f_2(x)(x - \alpha_2) \Rightarrow f(x) = f_2(x)(x - \alpha_1)(x - \alpha_2)$ con $grad(f_2) = n - 2$ y de forma inductiva tendremos que $f(x) = f_n(x)(x - \alpha_1)\cdots(x - \alpha_n)$ con $grad(f_n) = 0$ por tanto f queda factorizado linealmente.

$\therefore$ $\overline{F}$ es cerradura algebraica de F.

(*b*) En efecto, sabemos que $\mathbb{C} / \mathbb{Q}$ es una extensión de campo con $\mathbb{C}$ algebraicamente cerrado, por tanto por el inciso anterior $A / \mathbb{Q}$ es una extensión algebraica y en efecto es no finita pues $\mathbb{Q} \subseteq A$.

■

Problema 3. –

(2 puntos) Sea p un primo y K/E una extensión de campo de grado p. Sea $E \subseteq F \subseteq K$. Demuestra que $F = E$ ó $K = F$.

Demostración: Por la formula del grado (proposición 3.2.8) tenemos que como K / E es una extensión finita (pues su grado es p), entonces K / F y F / E también son extensiones finitas y además

$$[K : E] = [K : F][F : E] \Rightarrow p = [K : F][F : E]$$

pero como p es primo y el grado de una extensión es positivo, entonces $[K:F]=1$ y $[F:E]=p$ o $[K:F]=p$ y $[F:E]=1$. Recordando el problema 7 de la tercera lista de ejercicios si una extensión tiene grado 1 entonces ambos campos son isomorfos y en dado que caso que uno contenga al otro, estos serán iguales. Por tanto, en el primer caso $[K:F]=1$ y $[F:E]=p$ por lo que $K=F$ pues $F\subseteq K$, y en el segundo caso $[K:F]=p$ y $[F:E]=1$ por lo que $F=E$. En resumen $F=E$ o $K=F$.

■

Problema 4. –

(3 puntos) Sea K/F una extensión de campo de grado n.

a) Sea $c\in K$, demuestra que $T_c: K\to K$ definida como $T_c(k)=ck$ es una transformación F-lineal (tranformación lineal cuando pensamos a K como espacio vectorial sobre F).

b) Sea $M_n(F)$ el conjunto de las matrices de $n\times n$ con entradas en F. Demuestra que existe $K'\subseteq M_n(F)$ subanillo de $M_n(F)$ que es campo que extienda a F tal que $[K':F]=n$.

c) Demuestra que K es isomorfo (como campo) a K'. Concluye que $M_n(F)$ contiene una copia isomorfa de todas las extensiones de F de grado $\leq n$.

Demostración:

Corrección: En vez de $c\in K$ es $c\in F$ en la definición de la transformación lineal. En vez de $M_n(F)$ es $M_n(K)$. Creo que estas son correcciones al problema para que tenga sentido.

Recordando que K es un F-espacio vectorial con las operaciones de suma de K como campo y producto por escalar $f\cdot k=\varphi(f)k$ con $\varphi: F\to K$ isomorfismo. Además, es de dimensión finita n.

(a) Sea $c\in F$. Veamos que T_c es lineal.

• Sean $\lambda\in F$ y $a,b\in K$, entonces

$$T_c(\lambda\cdot a+b)=c\cdot(\lambda\cdot a+b)=\varphi(c)(\lambda a+b)=\varphi(c)(\varphi(\lambda)a+b)\underset{K \text{ campo}}{=}\varphi(c)\varphi(\lambda)a+\varphi(c)b$$
$$=\varphi(\lambda)[\varphi(c)a]+\varphi(c)b=\varphi(\lambda)[c\cdot a]+c\cdot b=\lambda\cdot[c\cdot a]+c\cdot b=\lambda\cdot T_c(a)+T_c(b)$$

por tanto, es lineal.

(b) Consideremos $A=\{[T_c]: c\in F\}\subseteq M_n(K)$ que está bien definido pues al ser K de dimensión n sobre F entonces la matriz asociada a T_c es de $n\times n$.

• A es subanillo de $M_n(K)$ con las operaciones heredadas.

- $T_0(v)=0_F\cdot v=\varphi(0)\cdot v=0_K\cdot v=0_K \Rightarrow [T_0]=0_{M_n(F)}\in A$

-Sean $[T_s],[T_r] \in A$ entonces

$$[T_s]-[T_r]=[T_s-T_r]=[T_{s+r}] \in A$$

la primera igualdad se da por propiedades de las matrices asociadas y la segunda es porque $T_s(v)+T_r(v)=sv+rv=(s+r)v=T_{s+r}(v)$.

-Sean $[T_s],[T_r] \in A$ entonces

$$[T_s][T_r]=[T_s \circ T_r]=[T_{sr}] \in A$$

la primera igualdad se da por propiedades de las matrices asociadas y la segunda es porque $T_s(T_r(v))=sT_r(v)=srv=T_{sr}(v)$.

Por tanto, es subanillo de $M_n(F)$.

• A es campo.

-Tenemos que $T_1(v)=1\cdot v=\varphi(1)\cdot v=1_K v=v$ por tanto $[T_1]=Id_{M_n(K)}$.

-Sea $[T_s] \in A$ distinto de cero, entonces

$$[T_s]^{-1}=[T_s{}^{-1}]=[T_{1/s}] \in A$$

esto es debido a dos razones: La primero, si $[T_s] \neq 0 \Rightarrow T_s(u) \neq 0$ para algún u elemento de la base, por lo que $0 \neq s\cdot u=\varphi(u)\cdot s$ y al ser K un campo, es dominio entero por lo que $s \neq 0$ y entonces $1/s \in K$. La segunda será consecuencia de lo anterior, como como $s \neq 0$ entonces $T^{-1}{}_s(v)$ es tal que $T_s{}^{-1}(T_s(v))=v \Rightarrow T_s{}^{-1}(sv)=v \Rightarrow T_s{}^{-1}(v)=\frac{1}{s}v=T_{1/s}(v)$ que está bien definido.

Por tanto, es campo.

• A es campo que extiende a F.

Como K extiende a F existe $\tilde{F} \subseteq K$ subcampo isomorfo a F, por lo que $\tilde{A}=\{[T_c]: c \in \tilde{F}\}$ es subcampo de A y además si $\psi: \tilde{F} \to \tilde{A}$ dada por $\psi(f)=[T_f]$ y veamos que es isomorfismo.

-Sean $f,g \in \tilde{F} \Rightarrow$

$$\psi(f+g)=[T_{f+g}] \underset{(b)}{=} [T_f+T_g]=[T_f]+[T_g]=\psi(f)+\psi(g)$$

-Sean $f,g \in \tilde{F} \Rightarrow$

$$\psi(fg) = [T_{fg}] \underset{(b)}{=} [T_f \circ T_g] = [T_f][T_g] \ = \psi(f)\psi(g)$$

Por tanto, es morfismo. Y al ser morfismo de campos entonces es inyectiva, solo basta probar que es suprayectiva. Sea $[T_c] \in \tilde{A}$, entonces $c \in \tilde{F}$ por lo que $\psi(c) = [T_c]$, por tanto, es suprayectiva. Con lo que ψ es un isomorfismo. Por tanto como $\tilde{A} \simeq \tilde{F} \simeq F$ entonces existe un subcampo de A isomorfo a F por tanto A / F es extensión de campos.

(*c*) Consideremos $\psi : K \to A$ dada por $\psi(k) = [T_{\varphi^{-1}(k)}]$ y veamos que es isomorfismo.

-Sean $k, t \in K \ \Rightarrow$

$$\psi(k+t) = [T_{\varphi^{-1}(k+t)}] \underset{\text{iso}}{=} [T_{\varphi^{-1}(k)+\varphi^{-1}(t)}] \underset{(b)}{=} [T_{\varphi^{-1}(k)} + T_{\varphi^{-1}(t)}] = [T_{\varphi^{-1}(k)}] + [T_{\varphi^{-1}(t)}] = \psi(k) + \psi(t)$$

-Sean $k, t \in K \ \Rightarrow$

$$\psi(kt) = [T_{\varphi^{-1}(kt)}] \underset{\text{iso}}{=} [T_{\varphi^{-1}(k)\varphi^{-1}(t)}] \underset{(b)}{=} [T_{\varphi^{-1}(k)} \circ T_{\varphi^{-1}(t)}] = [T_{\varphi^{-1}(k)}][T_{\varphi^{-1}(t)}] \ = \psi(k)\psi(t)$$

Por tanto, es morfismo. Y al ser morfismo de campos entonces es inyectiva, solo basta probar que es suprayectiva. Sea $[T_c] \in A$, entonces $c \in F$ por lo que si tomo $y = \varphi(c)$, entonces $\psi(y) = [T_{\varphi^{-1}(y)}] = [T_{\varphi^{-1}(\varphi(c))}] = [T_c]$, por tanto es suprayectiva. Con lo que ψ es un isomorfismo. Por tanto $K \simeq A$.

----No supe como concluir por falta de tiempo---

■