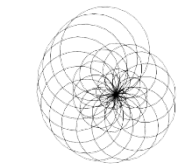

Universidad Nacional Autónoma de México
Facultad de Ciencias

Algebra Moderna II

3ra lista de ejercicios

Por: Lorenzo Antonio Alvarado Cabrera

CAMPOS

Problema 1. –
Sea K un campo y $S \subseteq K$. Entonces la intersección de todos los subcampos de K que contienen a S es un subcampo de K (que contiene a S).

Demostración: Sea $\overline{S} = \bigcap\{F \subseteq K : F \text{ subcampo y } S \subseteq F\}$, veamos que se cumple lo pedido.

- Como $0 \in F$ para cualquier subcampo de K entonces $0 \in \overline{S}$.
- Sean $a, b \in \overline{S}$ entonces $a, b \in F$ para todo F subcampo de K $\Rightarrow a - b \in F$ y por tanto $a - b \in \overline{S}$.
- Sean $a, b \in \overline{S}$, $b \neq 0$ entonces $a, b \in F$ para todo F subcampo de K $\Rightarrow ab^{-1} \in F$ y por tanto $ab^{-1} \in \overline{S}$.

Por estos tres puntos $\overline{S}$ es subcampo de K y además como para cada K, $S \subseteq K$ entonces $S \subseteq \bigcap\{F \subseteq K : F \text{ subcampo y } S \subseteq F\} = \overline{S}$.

■

Problema 2. –
Demuestra los detalles que nos faltaron para probar:

Si $(F, +_F, \cdot_F)$ es una extensión de campos de $(E, +_E, \cdot_E)$, entonces F es un E-espacio vectorial, es decir, un espacio vectorial sobre el campo E.

Demostración: Ya probamos todas las propiedades con la suma.
Como F es extensión de campos de E existe $\varphi : E \to F$ monomorfismo de anillos unitarios. Se define el producto por escalar como $\cdot : E \times F \to F$ dada por $e \cdot f = \varphi(e) \cdot f$. Veamos que se cumples las demás propiedades.

• Sean $a,b \in E$ y $f \in F$ entonces $a\cdot(b\cdot f) = a\cdot(\varphi(b)f) = \varphi(a)[\varphi(b)f] = [\varphi(a)\varphi(b)]f \underset{\text{morfismo}}{=} \varphi(ab)f$ $= (ab)\cdot f$, por lo que la operación es asociativa.

• El elemento 1_E es el neutro pues $1_E \cdot f = \varphi(1_E)f = 1_F f = f$.

• Sean $a \in E$ y $f,g \in F$ entonces $a\cdot(f+g) = \varphi(a)(f+g) = \varphi(a)f + \varphi(a)g = a\cdot f + a\cdot g$ por lo tanto se distribuye en la suma.

• Finalmente, sean $a,b \in E$ y $f \in F$ entonces $(a+b)\cdot f = \varphi(a+b)f = [\varphi(a)+\varphi(b)]f = \varphi(a)f + \varphi(b)$ $= a\cdot f + b\cdot f$ por lo tanto se distribuye en la suma de escalares.

Por lo tanto, es E-espacio vectorial.

■

Problema 3. –

Sean F un campo, A un anillo y $f : F \to A$ un morfismo de anillos. Demuestra que si f es no cero, entonces f es monomorfismo.

Demostración: Sabemos que $\ker(f)$ es un ideal de F y al ser F un campo, sus únicos ideales son $\{0\}$ o F, por lo que $\ker(f) = \{0\}$ o F, pero no puede pasar que $\ker(f) = F$ pues significaría que $\forall a \in F,\ f(a) = 0 \Rightarrow f \equiv 0$!!! pero por hipótesis esto no pasa. Entonces $\ker(f) = \{0\}$ por lo que es inyectiva y por tanto, monomorfismo.

■

Problema 4. –

a) Sea F un campo finito de orden q y sea $f(x)$ un polinomio irreducible en $F[x]$ de grado $n \geq 1$. Demuestra que $F[x]/\langle f(x)\rangle$ tiene q^n elementos.

b) Deduce que si $p \in \mathbb{Z}$ es primo y $n \in \mathbb{N}$ es no cero, entonces podemos construir un campo con p^n elementos.

Demostración:

(a)

Problema 5. –

Demuestra que $\mathbb{R}[x]_{/<x^2+1>}$ *es un campo isomorfo a* $\mathbb{C}$

Demostración: Sabemos que $\mathbb{C}/\mathbb{R}$ es una extensión de campo y $i \in \mathbb{C}$ es un elemento algebraico sobre $\mathbb{R}$, pues $p(x) = x^2 + 1 \in \mathbb{R}[x]$ es tal que es monico y $p(i) = 0$. Mas aún, $p(x)$ es irreducible pues si $q(x), r(x) \in \mathbb{R}[x]$ no unidades, son tales que $p(x) = q(x)r(x) \Rightarrow 0 = q(i)r(i)$ y entonces si suponemos que $q(i) = 0$, dado que necesariamente $grad(q) = 1$, entonces

$a(i)+b=0 \Leftrightarrow\ b=-ai$ lo cual es imposible pues $a,b\in\mathbb{R}$ por lo tanto no puede pasar que $q(i)=0$, análogamente para $r(x)$ por lo cual uno de los dos tiene que ser unidad, es decir, $p(x)$ es irreducible.

Con esto tendremos por el Teorema 3.3.6 tendremos que existe un isomorfismo $\varphi:\mathbb{R}[x]_{/<p(x)>}\to\mathbb{R}(i)$, y como $\mathbb{R}(i)=\{a+ib:a,b\in\mathbb{R}\}=\mathbb{C}$ entonces tenemos un isomorfismo entre $\mathbb{R}[x]_{/<x^2+1>}$ y $\mathbb{C}$, por tanto, $\mathbb{R}[x]_{/<x^2+1>}\simeq\mathbb{C}$.

(Esto es pues por el Teorema 3.2.12 $\mathbb{R}[x]_{/<x^2+1>}$ es campo.)

■

Problema 6. –

Describe todos los ideales del anillo $F[x]/\langle f(x)\rangle$, donde F es un campo y $f(x)\in F[x]$.

Sugerencia: Decríbelos en términos de la factorización de $f(x)$.

Demostración:

Problema 7. –

Demuestra que E es una extensión de grado 1 de F, si y sólo si, $F\simeq E$.

Demostración: Recordemos que si E es una extensión de F existe $\tilde{F}\simeq F$ subcampo de E.

$\Rightarrow$] Vamos a demostrar que $E=\tilde{F}$.
Supongamos que $[E:F]=1\Rightarrow\ [E:\tilde{F}]=1$ y por contradicción supongamos que $\tilde{F}\neq E$, entonces necesariamente $\tilde{F}\subset E$, entonces sea $e\in E\backslash\tilde{F}$ que será un elemento algebraico sobre $\tilde{F}$ (ya que la extensión es finita $\Rightarrow$ algebraica) por lo que por el teorema 3.3.6 existe $p(x)\in\tilde{F}[x]$ monico e irreducible tal que $p(e)=0$, por otro lado, sabemos que $\tilde{F}\subseteq\tilde{F}(e)\subseteq E$ y entonces por la proposición 3.2.8 tendremos

$$1=[E:\tilde{F}]=[E:\tilde{F}(e)][\tilde{F}(e):\tilde{F}]\ \Leftrightarrow\ [E:\tilde{F}(e)]=[\tilde{F}(e):\tilde{F}]=1$$

entonces $grad(p(x))=[\tilde{F}(e):\tilde{F}]=1\ \Rightarrow p(x)=ax+b$ con $a,b\in\tilde{F}$, entonces $p(e)=0\ \Leftrightarrow$ $ae+b=0_{\tilde{F}}\underset{F\text{ campo}}{\Leftrightarrow}\ e=-ba^{-1}\in\tilde{F}$ por lo tanto $e\in\tilde{F}$!!! esto contradice el hecho de que $e\in E\backslash\tilde{F}$ por tanto $E=\tilde{F}\simeq F$.

$\Leftarrow$] Supongamos que $F \simeq E$, entonces E es un subcampo isomorfo a F de E por lo que E es extensión de campos de F. Además para cada $e \in E$ existe un único $\tilde{e} \in F$ tal que $\varphi(\tilde{e}) = e$, por lo que $E = \{e : e \in E\} = \{e1_E : e \in E\} = \{\varphi(\tilde{e})1_E : \tilde{e} \in F\} = \{\tilde{e} \cdot 1_E : \tilde{e} \in F\} =< \{1_E\} >$ por tanto $\dim_F E = 1$, es decir, $[E : F] = 1$.

■

Problema 8. –

Da un ejemplo de dos campos K y F tales que K sea una extensión finita de F, pero F no sea una extensión de K.

Deduce que la relación K es extensión finita de F no es una relación de equivalencia.

Demostración: Sea $K = \mathbb{C}$ y $F = \mathbb{R}$, tenemos por lo visto en clase que $[\mathbb{C} : \mathbb{R}] = 2 < \infty$ es una extensión finita, pero $\mathbb{R}$ no es extensión de $\mathbb{C}$ ya que si lo fuera tendríamos que $[\mathbb{C} : \mathbb{C}] = [\mathbb{C} : \mathbb{R}][\mathbb{R} : \mathbb{C}] \Rightarrow 1 = 2[\mathbb{R} : \mathbb{C}]$!!!

Por tanto, la relación de extensión finita no es de equivalencia pues no se cumple la propiedad simétrica.

■

Problema 9. –

Sea E/F una extensión del campo F y sea $\alpha \in E$. Muestra que α es algebraico sobre F si, y sólo si, $F(\alpha)$ es una extensión finita de F.

Demostración:

$\Rightarrow$]Sea da por el teorema 3.3.6.

$\Leftarrow$] Supongamos que $[F(\alpha) : F] = n < \infty$, entonces es una extensión algebraica, por lo que $\forall f \in F(\alpha)\ \exists p(x) \in F[x]$ tal que $p(f) = 0$, en particular $\alpha \in E \subseteq F(\alpha)$ por lo que $\exists p(x) \in F[x]$ tal que $p(\alpha) = 0$, entonces α es algebraico sobre F.

■

Problema 10. –

Sea $F(\alpha)$ extensión simple finita de F y $p(x)$ es el polinomio irreducible de α sobre F. Si α no es raíz de $f(x) \in F[x]$.

a) Demuestra que $p(x)$ no divide a $f(x)$;
b) Concluye que $(p(x), f(x)) = 1$;
c) Deduce que existe un polinomio $a(x)$ en $F[x]$ tal que $a(\alpha)$ es el inverso multiplicativo de $f(\alpha) \in F[\alpha]$;
d) Concluye que los incisos anteriores proveen un algoritmo para encontrar el inverso de un elemento (no nulo) en $F[\alpha]$.

Demostración: Podemos considerar a $p(x)$ monico sin pérdida de generalidad.

(*a*) En efecto, si pasara que $p(x) \mid f(x)$ entonces existiría $q(x) \in F[x]$ tal que $f(x) = p(x)q(x)$ y entonces $f(\alpha) = p(\alpha)q(\alpha) = 0q(\alpha) = 0$!!!, esto contradice que α no es raíz de $f(x)$, por tanto, $p(x) \nmid f(x)$.

(*b*) Sea $d(x) = (p(x), f(x))$, entonces $d(x) \mid p(x)$ y $d(x) \mid f(x)$, pero si $d(x) \mid p(x) \Rightarrow p(x) = q(x)d(x)$ y al ser $p(x)$ irreducible entonces $q(x)$ o $d(x)$ es unidad. Si $d(x)$ es unidad entonces $d(x) = d \in F$ por lo que $d \mid p(x)$ pero al ser $p(x)$ monico la única posibilidad es que $d = 1$. Si $q(x)$ es unidad, entonces $q(x) = q \in F$ por lo que $p(x) = qd(x)$ y nuevamente $q \mid p(x)$ por lo que $q = 1$ entonces $p(x) = d(x)$, pero de ser el caso tendríamos que $p(x) \mid f(x)$ lo cual no pasa, entonces la única posibilidad es que $d = 1$.

(*c*) Por los incisos anteriores como $p(x) \nmid f(x)$ y $(p(x), f(x)) = 1$ entonces $f(x) \nmid p(x)$ pues de hacerlo tendríamos que $(p(x), f(x)) \neq 1$, de esta manera por el algoritmo de la división existen $q(x), r(x) \in F[x]$ con $0 \neq r(x)$ y $\text{grad}(r(x)) < \text{grad}(f(x))$ tal que $p(x) = q(x)f(x) + r(x)$, entonces nuevamente por el algoritmo de la división aplicado a $r(x)$ con $q(x)$ (pues $r(x) \neq 0$) existen $q_1(x), r_1(x) \in F[x]$ con $0 = r_1(x)$ o $\text{grad}(r_1(x)) < \text{grad}(r(x))$ tal que $q(x) = q_1(x)r(x) + r_1(x)$.
Si $0 = r_1(x)$ entonces $q(x) = q_1(x)r(x)$, por lo que $p(x) = q_1(x)r(x)f(x) + r(x) = r(x)[q_1(x)f(x) + 1]$ entonces $0 = r(\alpha)[q_1(\alpha)f(\alpha) + 1]$

⊙ Si $r(\alpha) = 0$, entonces $p(\alpha) = q(\alpha)f(\alpha) + r(\alpha) \Rightarrow 0 = q(\alpha)f(\alpha)$

……..

Problema 11. –
Considera $\alpha = 2^{1/2} + 3^{1/2}$. Usando el hecho que $p(x) = x^4 - 10x^2 + 1$ es el polinomio irreducible de α. Calcula α^{-1}.

Sugerencia: Sustituye α en $p(x)$ y factoriza α.

Demostración: