Quiz 2 Algebra Moderna

Daniel Fabian Osorio Valencia, Código: 8946508

October 2020

1 Punto 1:

Sea A un anillo conmutativo unitario y sea M un ideal de A. Demuestre que A/M es cuerpo si, y solamente si, M es maximal.

1.1 Lemas auxiliares:

Lema 1. Para todo anillo cociente R/I, el cero de este es de la forma $0 + I$ siendo 0, el cero en R.

Prueba: Por ver que para todo $x \in R$, se cumple que $x(0 + I) = (0 + I)x = (0 + I)$. Sea entonces $x \in R/I$ de la forma $x = r + I$ con $r \in R$:

$$\begin{aligned} &(r + I)(0 + I) \\ &\quad (r0) + I \text{ (propiedad anillo cociente)} \\ &\quad\quad 0 + I \text{ (producto cero en } R) \end{aligned} \qquad \square$$

por el otro lado se tiene que:

$$\begin{aligned} &(0 + I)(r + I) \\ &\quad (0r) + I \text{ (propiedad anillo cociente)} \\ &\quad\quad 0 + I \text{ (producto cero en } R) \end{aligned} \qquad \square$$

Lema 2. Para todo anillo cociente R/I, el elemento unitario de este es de la forma $1 + I$ siendo 1, el elemento unitario en R.

Prueba: Por ver que para todo $x \in R$, se cumple que $x(1 + I) = (1 + I)x = x$. Sea entonces $x \in R/I$ de la forma $x = r + I$ con $r \in R$:

$$\begin{aligned} &(r + I)(1 + I) \\ &\quad (r1) + I \text{ (propiedad anillo cociente)} \\ &\quad\quad r + I \text{ (identidad en } R) \end{aligned} \qquad \square$$

por el otro lado se tiene que:

$$\begin{aligned}(1+I)(r+I)\\ (1r)+I \text{ (propiedad anillo cociente)}\\ r+I \text{ (identidad en } R)\end{aligned} \qquad \square$$

Lema 3. Para todo anillo cociente R/I con $x, y \in R$ se cumple que si $x+I=y+I$ entonces $x-y \in I$

Prueba: Sea entonces $x, y \in R$:

$$\begin{aligned}x+I &= y+I \text{ (hipotesis)}\\ (x+I)+(-y+I) &= (y+I)+(-y+I) \text{ (ley de uniformidad)}\\ (x-y)+(I+I) &= (y-y)+(I+I) \text{ (Asociativa y conmutativa en } R)\\ (x-y)+I &= 0+I \text{ (Invertiva en } R \text{ y clausurativa en } I)\\ (x-y)+I &= I \text{ (modulativa en } R)\\ (x-y) &\in I \text{ (clausurativa en } I)\end{aligned} \qquad \square$$

1.2 Prueba $\Rightarrow$:

Sea A un anillo conmutativo unitario, sea M un ideal de A y sea A/M un cuerpo. Por ver que M es maximal, es decir, que para todo ideal I de A tal que $M \subseteq I \subseteq A \wedge M \neq I$, entonces $I=A$. Sea entonces I un ideal de A tal que $M \subseteq I \subseteq A \wedge M \neq I$. Como $M \subseteq I \wedge M \neq I$, entonces existe un $x \in I \wedge x \notin M$. Ahora como $x \notin M$ entonces:

$$\begin{aligned}x+M &\neq M\\ x+M &\neq M+0 \text{ (identidad en M)}\end{aligned}$$

Ahora como $x \in I \wedge I \subseteq A$ entonces $x \in A$, y como $x \in A$ por definicion de A/M entonces $x+M \in A/M$. Ademas como $x+M \neq M+0$ y por el lema 1 se sabe que $x+M$ es diferente del cero de A/M. De este modo, como $x+M$ es diferente del cero de A/M y por hipotesis A/M es cuerpo, entonces $x+M$ tiene un inverso $y+M$ tal que al operarlos da la identidad de A/M (lema 2):

$$\begin{aligned}(x+M)(y+M) &= 1+M\\ (xy)+M &= 1+M \text{ (propiedad anillo cociente)}\\ xy-1 &\in M \text{ (lema 3)}\end{aligned}$$

Como $xy - 1 \in M$ y $M \subseteq I$, entonces $xy - 1 \in I$. Teniendo esto en cuenta se tiene que:

$$1 = xy - (xy - 1) \wedge xy - 1 \in I \wedge x \in I \wedge y \in A$$
$$1 = xy - (xy - 1) \wedge xy - 1 \in I \wedge xy \in I \text{ (absorbcion en I)}$$
$$1 = xy - (xy - 1) \in I \text{ (clausurativa en I)}$$
$$1 \in I$$

Finalmente se tiene que para todo $a \in A$:

$$a = a1 = 1a \wedge 1 \in I$$
$$a = a1 = 1a \in I \text{ (absorbcion I)}$$

por lo cual I = A. □

1.3 Prueba $\Leftarrow$:

Sea A un anillo conmutativo unitario, sea M un ideal de A y sea M maximal. Por ver que A/M es un cuerpo, es decir, que A/M es un anillo unitario conmutativo en el cual todo elemento diferente de 0 tiene inverso.

1.3.1 A/M es un anillo unitario:

Por lema 2 se sabe que el uno de A/M es $1 + M$ con 1 siendo el 1 de A, y como A es unitario por hipotesis, entonces $1 \in A$, por lo cual por definicion de A/M, $1 + M \in A/M$. □

1.3.2 A/M es un anillo conmutativo:

Por ver que para todo $a + M, b + M \in A/M$, entonces $(a + M)(b + M) = (b + M)(a + M)$. Sea entonces $a + M, b + M \in A/M$:

$$(a + M)(b + M) = ab + M \text{ (propiedad anillo cociente)}$$
$$(a + M)(b + M) = ba + M \text{ (conmutativa en A)}$$
$$(a + M)(b + M) = (b + M)(a + M) \text{ (propiedad anillo cociente)} \qquad \square$$

1.3.3 Todos los $x \in A/M$ donde $x \neq 0$ tienen inverso:

Sea $a + M \in A/M$ y sea $a + M$ diferente del cero de A/M, es decir:

$$a + M \neq 0 + M \text{ (lema 1)}$$
$$a + M \neq M \text{ (identidad en M)}$$

Como $a + M \neq M$, quiere decir que $a \notin M$, ya que si $a \in M$ entonces $M + a = M$ por clausurativa en M. Se considera ahora el subconjunto de J que utiliza el a mencionado anteriormente de la forma $J = M + Aa = \{m + ba | b \in A \wedge m \in M\}$. A continuacion se demostrara que J es un ideal de A:

Lemma 4. J es un ideal de A.

Prueba: Inicialmente se sabe que $J \subseteq A$, ya que $J = M + Aa$ y $M \subseteq A \wedge a \in A$, por lo cual por cerradura en A, $M + Aa \in A$. Queda entonces por ver que J es subgrupo aditivo de A, es decir que para todo $x, y \in J$ se cumple que $xy^{-1} \in J$, en este caso (+), que $x - y \in J$. Finalmente se debe demostrar la absorbcion para J, es decir, que para todo $b \in A \wedge j \in J$ se cumple que $jb \in J \wedge bj \in J$. Sea entonces $x, y \in J$:

$$x - y = (m_1 + b_1 a) - (m_2 + b_2 a) \wedge m_1, m_2 \in M \wedge b_1, b_2 \in A$$
$$x - y = m_1 + b_1 a - m_2 - b_2 a \wedge m_1, m_2 \in M \wedge b_1, b_2 \in A \text{ (aritmetica)}$$
$$x - y = (m_1 - m_2) + (b_1 a - b_2 a) \wedge m_1, m_2 \in M \wedge b_1, b_2 \in A \text{ (conmutativa, asociativa en A)}$$
$$x - y = (m_1 - m_2) + a(b_1 - b_2) \wedge m_1, m_2 \in M \wedge b_1, b_2 \in A \text{ (distributiva en A)}$$
$$x - y = (m_3) + a(b_3) \wedge m_3 \in M \wedge b_3 \in A \text{ (cerradura en A y en M)}$$
$$x - y = (m_3) + a(b_3) \in J \text{ (def J)}$$

Ahora para verificar absorbcion, sea $j \in J$ y $b_2 \in A$:

$$jb_2 = (m_1 + b_1 a)b_2 \wedge m_1 \in M \wedge b_1 \in A$$
$$jb_2 = m_1 b_2 + b_1 a b_2 \wedge m_1 \in M \wedge b_1 \in A \text{ (distributiva A)}$$
$$jb_2 = m_1 b_2 + b_1 b_2 a \wedge m_1 \in M \wedge b_1 \in A \text{ (conmutativa A)}$$
$$jb_2 = m_2 + b_3 a \wedge m_2 \in M \wedge b_3 \in A \text{ (absorbcion M y clausurativa A)}$$
$$jb_2 = m_2 + b_3 a \in J \text{ (def J)}$$

Del otro lado:

$$b_2 j = b_2(m_1 + b_1 a) \wedge m_1 \in M \wedge b_1 \in A$$
$$b_2 j = b_2 m_1 + b_2 b_1 a \wedge m_1 \in M \wedge b_1 \in A \text{ (distributiva A)}$$
$$b_2 j = m_2 + b_3 a \wedge m_2 \in M \wedge b_3 \in A \text{ (absorbcion M y clausurativa A)}$$
$$b_2 j = m_2 + b_3 a \in J \text{ (def J)}$$

Al verificarse que J es subgrupo aditivo de A y que J cumple la absorbcion, se concluye que J es ideal de A. $\square$

Siguiendo con la prueba, $M \subseteq J$, ya que para todo $m \in M$, $m \in J$ de la forma $m + 0a = m + 0 = m$. Ademas, $a \in J$ de la forma $0 + 1a = 1a = a$, pero como se habia dicho antes, $a \notin M$, por lo cual si $a \in J \wedge a \notin M$ entonces $M \neq J$, y como $M \neq J \wedge M \subseteq J \wedge$ J es ideal de A, por definicion de maximal, $J = A$. Ahora como A es unitario y $J = A$, entonces el 1 en A se puede escribir como:

$$1 = m + ba \wedge m \in M \wedge b \in A$$

Tomando en cuenta esto, el 1 en A/M por lema 2 y la igualdad anterior seria:

$1 + M = (m + ba) + M \wedge m \in M \wedge b \in A$

$1 + M = ba + M \wedge m \in M \wedge b \in A$ (conmutativa, asociativa en A y clausurativa en M)

$1 + M = (b + M)(a + M) \wedge m \in M \wedge b \in A$ (propiedad anillo cociente)

Por lo cual, para todo elemento $x \in A/M$ de la forma $a + M$ con $a + M \neq 0 + M$, existe un $x^{-1} = (b + M)$ tal que $(b + M)(a + M) = 1 + M$. $\square$

Al cumplirse las 3 condiciones para que A/M sea cuerpo, se concluye que A/M es cuerpo. $\square$

2 Punto 2:

Provee un ejemplo de aplicacion del resultado anterior que no este relacionado con los ejemplos que hemos venido trabajando en clase, en los temas referentes a ideales.

2.1 Ejemplo:

Sea F un campo, sea $p(x) \in F[x]$ un polinomio irreducible y sea $\langle p(x) \rangle = \{f(x)p(x) | f(x) \in F[x]\}$, el ideal principal generado por $p(x)$. Entonces $F[x]/\langle p(x) \rangle$ es un campo.

2.2 Lemas auxiliares:

Lema 5. Si F es un campo, entonces todos los ideales de $F[x]$ son ideales principales.

Prueba: Por ver que todo ideal de $F[x]$ es de la forma $\langle p(x) \rangle = \{f(x)p(x) | f(x) \in F[x]\}$. Por definicion de campo se sabe que F es un dominio entero y por observacion se sabe que si un anillo A es dominio entero, entonces $A[x]$ es dominio entero, por lo cual, $F[x]$ es un dominio entero. Considerando el caso en que el ideal $I = \{0\}$, entonces I es principal de la forma $\langle 0 \rangle = \{f(x)0 | f(x) \in F[x]\}$. De otro lado, si $I \neq \{0\}$ entonces sea un elemento $p(x) \in I$ de grado minimo con $p(x) \neq 0$ y sea $f(x) \in I$. Ahora por algoritmo de la division se sabe que existen $q(x), r(x)$ tal que $f(x) = q(x)p(x) + r(x)$ con $r(x) = 0$ o $gr(r(x) < gr(p(x))$. Pero $gr(r(x) < gr(p(x))$ no es cierto ya que $r(x) = f(x) - q(x)p(x)$ y $gr(p(x))$ es minimo, por lo cual $r(x) = 0$. De esta forma, $f(x) = q(x)p(x)$ por lo cual, por definicion de $\langle p(x) \rangle$, $f(x) \in \langle p(x) \rangle$. $\square$

2.3 Demostracion:

Se quiere demostrar por el teorema anteriormente visto que $F[x]/\langle p(x)\rangle$ es campo, por lo cual, por ver que $\langle p(x)\rangle$ es maximal y $F[x]$ es un anillo conmutativo unitario.

2.3.1 $F[x]$ es un anillo conmutativo unitario:

Si F es un campo, entonces por definicion de campo se sabe que F es un anillo conmutativo y unitario. De este modo por observaciones se sabe que para todo anillo A, si este es conmutativo entonces A[x] es conmutativo y de igual forma si A es unitario, entonces $A[x]$ es unitario, por lo cual es posible concluir que por ambas observaciones, $F[x]$ es un anillo unitario y conmutativo. $\square$

2.3.2 $\langle p(x)\rangle$ es maximal:

Por ver que para todo ideal I de $F[x]$ tal que $\langle p(x)\rangle \subseteq I \subseteq F[x]$, entonces $I = F[x] \vee I = \langle p(x)\rangle$. Inicialmente, por lema 5 se sabe que $I = \langle f(x)\rangle$ donde $f(x) \in F[x]$, por lo cual $\langle p(x)\rangle \subseteq \langle f(x)\rangle \subseteq F[x]$. Ahora como $\langle p(x)\rangle \subseteq \langle f(x)\rangle$, entonces $p(x) \in \langle f(x)\rangle$, por lo cual por definicion de $\langle f(x)\rangle$, $p(x) = a(x)f(x)$ con $a(x) \in F[x]$. Ahora, por hipotesis $\langle p(x)\rangle$ es irreducible, por lo cual $a(x)$ es una constante o $f(x)$ es una constante, ambas distintas de cero. En caso de que $a(x)$ sea constante, entonces $\langle p(x)\rangle = \langle f(x)\rangle$, y si $f(x)$ es constante, entonces $\langle f(x)\rangle = F[x]$. $\square$

Al probar que se cumplen las condiciones de que $F[x]$ es un anillo conmutativo unitario y que $\langle p(x)\rangle$ es maximal de $F[x]$, se concluye por el teorema que $F[x]/\langle p(x)\rangle$ es un cuerpo. $\square$