

AYUDANTÍA I

ÁLGEBRA I POSTGRADO (OTOÑO 2017)

En esta ayudantía estudiaremos la parte básica de la teoría de cuerpos.

1.- Problema 1:

Sea A un dominio de integridad.

- i.- Pruebe que si A es finito entonces A es un cuerpo.
- ii.- Muestre que para todo $z \in \mathbb{Z}[i]$ se cumple que $\mathbb{Z}[i]/(z)$ es un cuerpo o no es un dominio de integridad.

Desarrollo:

- i.- Debemos probar que todo elemento no nulo en A tiene un inverso multiplicativo. Sea $x \in A - \{0\}$ y considere $\phi : A \rightarrow A$ el homomorfismo de grupos definido por $\phi(a) = ax$. Note que $\ker(\phi) = \{a \in A : ax = 0\} = \{0\}$, ya que A es un DI. Como $(A, +)$ es un grupo finito concluimos que ϕ es un isomorfismo. En particular, ϕ es sobreyectivo. Por lo tanto existe $y \in A$ tal que $xy = yx = 1$.
- ii.- Recordemos que para todo $z \in \mathbb{Z}[i]$ el cociente $\mathbb{Z}[i]/(z)$ es finito. De hecho, se puede demostrar que $|\mathbb{Z}[i]/(z)| = N(z)$. Aplicando [i] se obtiene lo pedido. Otra forma de demostrar este hecho, es recordar que $\mathbb{Z}[i]$ es un DIP. Luego si $\mathbb{Z}[i]/(z)$ es un dominio de integridad, se tiene que (z) es un ideal primo, luego un ideal maximal. De esto se sigue que $\mathbb{Z}[i]/(z)$ es un cuerpo.

2.- Problema 2:

Sea $\mathbb{F}_p$ el cuerpo de p elementos.

- i.- Demuestre que la función $x \mapsto x^p - x$ es nula en $\mathbb{F}_p$.
- ii.- Concluya que el polinomio $p(x) = x^p - x$ es no nulo y se factoriza en producto de polinomios lineales en $\mathbb{F}_p$.

Desarrollo:

- i.- Basta probar que para todo $x \in \mathbb{F}_p$ se tiene que $x^p = x$. Para probar esto, observe que $(\mathbb{F}_p^*, \cdot)$ es un grupo finito de cardinal $p - 1$. Luego, por teorema de Lagrange, tenemos que para todo $x \in \mathbb{F}_p^*$ se tiene que $x^{p-1} = 1$. Esto implica que $x^p = x$, para todo $x \in \mathbb{F}_p$.
- ii.- Dado que $p(x)$ tiene coeficientes no nulos, se tiene que $p(x)$ es un polinomio no nulo. Por otro lado, como $p(x)$ es un polinomio de grado p que tiene p raíces distintas en $\mathbb{F}_p$, se tiene que $p(x) = \prod_{a \in \mathbb{F}_p} (x - a)$.

3.- Problema 3:

Sea $F = \mathbb{Q}(\sqrt[n]{2})$ el mínimo cuerpo contenido en $\mathbb{R}$ que contiene a $\mathbb{Q}$ y $\sqrt[n]{2}$. Demuestre que $F = \{a_0 + a_1 \sqrt[n]{2} + \cdots + a_{n-1} \sqrt[n]{2^{n-1}} : a_i \in \mathbb{Q}\}$. Determine $[F : \mathbb{Q}] = \dim_{\mathbb{Q}} F$.

Desarrollo: Sea $X = \{a_0 + a_1 \sqrt[n]{2} + \cdots + a_{n-1} \sqrt[n]{2^{n-1}} : a_i \in \mathbb{Q}\}$. Como $\sqrt[n]{2} \in L$, es fácil demostrar que $X \subset L$. Luego, para demostrar que $L = X$, basta demostrar que X es un cuerpo. Esto ya que, como $\sqrt[n]{2} \in X$ y $\mathbb{Q} \subset X$ se tiene que $X \supset L$. En lo que sigue demostraremos que X es un cuerpo. Sea $\phi : \mathbb{Q}[x] \rightarrow X$ el homomorfismo de anillos definido por $\phi(x) = \sqrt[n]{2}$. Claramente ϕ es sobreyectivo y $p(x) = x^2 - 2 \in \ker(\phi)$. Note que por criterio de Eisenstein, se tiene que $p(x)$ es irreducible. Dado que $\mathbb{Q}[x]$ es un DIP, podemos suponer que $\ker(\phi) = (p(x))$. Entonces $p(x) = s(x)t(x)$, para cierto $t(x) \in \mathbb{Q}[x]$. Como $p(x)$ es irreducible, tenemos que $t(x) \in \mathbb{Q}$ y en particular $(p(x)) = \ker(\phi)$. Concluimos que $X \cong \mathbb{Q}[x]/(p(x))$ es un cuerpo. Para calcular $[F : \mathbb{Q}]$ note que $\{1, \sqrt[n]{2}, \dots, \sqrt[n]{2^{n-1}}\}$ es una base de X como $\mathbb{Q}$ espacio vectorial. Esto pues claramente genera el espacio y sus elementos son linealmente independientes, debido a que si no, existiría un polinomio de grado menor a $p(x)$ que se anula en $\sqrt[n]{2}$, lo que contradice el hecho de que $\ker(\phi) = (p(x))$. Se sigue que $[F : \mathbb{Q}] = \dim_{\mathbb{Q}} F = n$.

4.- Problema 4:

Sea $p(x) = x^3 + 12x + 3 \in \mathbb{Q}[x]$ y θ una raíz de $p(x)$. Sea $\mathbb{Q}(\theta) \cong \mathbb{Q}[x]/(p(x))$ el mínimo cuerpo contenido en $\mathbb{C}$ que contiene a $\mathbb{Q}$ y θ .

- i.- Exprese $(\theta^2 + \theta + 5)(\theta + 3)$ en términos de $\{1, \theta, \theta^2\}$.
- ii.- Exprese $(\theta^2 + 3)^{-1}$ en términos de $\{1, \theta, \theta^2\}$.

Desarrollo:

- i.- Note que $a = (\theta^2 + \theta + 5)(\theta + 3) = \theta^3 + 4\theta^2 + 8\theta + 15$. Luego una preimagen de a por el homomorfismo ϕ , definido en [3], es $r(x) = x^3 + 4x^2 + 8x + 15$. Note que $r(x) = p(x) + 4x^2 - 4x + 12$. Por lo tanto, si evaluamos la igualdad anterior en $x = \theta$ obtenemos que $a = 4\theta^2 - 4\theta + 12$.
- ii.- Por un argumento análogo al mostrado en [3], debemos encontrar un polinomio $f(x)$ tal que $f(\theta)(\theta^2 + 3) = 1$. Tomando preimagenes vía ϕ , deducimos que debemos encontrar $f(x), g(x) \in \mathbb{Q}[x]$ tales que $(x^2 + 3)f(x) + p(x)g(x) = 1$. Para encontrar dichos polinomios, debemos aplicar algoritmo de división. En efecto tenemos que:

$$\begin{aligned} p(x) &= x(x^2 + 3) + (9x + 3), \\ x^2 + 3 &= \frac{x}{9}(9x + 3) + \left(3 - \frac{1}{3}x\right), \\ 9x + 3 &= -27\left(-\frac{1}{3}x + 3\right) + 84. \end{aligned}$$

Luego $84 = (x^2 + 3)(27 - x + \frac{1}{9}x^2) + (1 - \frac{1}{9}x)p(x)$. Evaluando en θ , concluimos que $(\theta^2 + 3)^{-1} = \frac{1}{84}(27 - \theta + \frac{1}{9}\theta^2)$.

Por Claudio Bravo Castillo.