Problemas de Ecuaciones Algebraicas

Rafael Arquero Gimeno @_arkeros
Helena Garví Casas

29 de octubre de 2015

Índice

Índice de figuras

Índice de cuadros

1. Grupos

1. Sea $f(X) = a_0 + a_1X + ... + a_nX^n \in \mathbb{Z}[X], a_0, ..., a_n \in \mathbb{Z}$, un polinomio. Supongamos $\exists p \in \mathbb{Z}$ primo tal que

$$p \nmid a_n, p^2 \nmid a_0, p \mid a_i \forall i = 0, ..., n-1 \tag{1}$$

Demostrad que f es irreductible en $\mathbb{Q}$. Si además f es primitivo, entonces tambien es irreductible en $\mathbb{Z}[X]$.

2. (Criterio de Eisenstein) Sean A un dominio de factorización unica, K su cuerpo de fracciones y $f(X) = a_0 + a_1X + ... + a_nX^n \in A[X], a_0, ..., a_n \in A$, un polinomio. Supongamos que $\exists p \in A$ primo tal que

$$p \nmid a_n, p^2 \nmid a_0, p \mid a_i \forall i = 0, ..., n-1 \tag{2}$$

Demostrad que f es irreductible en $K[X]$. Si además f es primitivo, entonces tambien es irreductible en $A[X]$.

3. Sean A, B dominios y $f : A \to B$ un morfismo de anillos. Denotamos por $\widetilde{f} : A[X] \to B[X]$ el morfismo de anillos dado por

$$\widetilde{f}(\sum_i a_iX^i) = \sum_i f(a_i)X^i, a_i \in A \tag{3}$$

   (a) Supongamos que A es un dominio de factorización unica. Demostrad que si $p(X) \in A[X]$ es un polinomio primitivo y $\widetilde{f}(p(X)) \in B[X]$ es irreductible y del mismo grado que $p(X) \in A[X] \implies p(X)$ es irreductible en $A[X]$.

   (b) Supongamos que $f : A \to B$ es un isomorfismo de anillos. Demostrad que $p(X) \in A[X]$ es irreductible $\iff \widetilde{f}(p(X))$ es irreductible en $B[X]$.

   (c) Dado $a \in A$, el polinomio $p(X) \in A[X]$ es irreductible $\iff p(X + a)$ es irreductible.

4. (Criterio de reducción)

   (a) Sean A, B dominios de integridad, L el cuerpo de fracciones de B y $f : A \to B$ un morfismo de anillos cualquiera. Llamamos $\widetilde{f} : A[X] \to B[X]$ el morfismo de anillos que se obtiene al aplicar f a los coeficientes de los polinomios de $A[X]$. Sea $p(X) \in A[X]$ un polinomio tal que $\widetilde{f}(p(X))$ es irreductible en $L[X], p(X)$ no admite ninguna factorización en $A[X]$ de la forma

   (b)

5. Construid las tablas de sumar y de multiplicar de los cuerpos $\mathbb{F}_n$, $\forall n \leq 10$. Explicitad generadores de los grupos multiplicativos.

Solución:

1. $\mathbb{F}_1$

$+$	0
0	0

$\times$	0
0	0

2. $\mathbb{F}_2$

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

3. $\mathbb{F}_3$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

4. $\mathbb{F}_4$

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\times$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

5. $\mathbb{F}_5$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
1	4	0	1	2	3

$\times$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

6. $\mathbb{F}_6$ No existe
7. $\mathbb{F}_7$
8. $\mathbb{F}_8$
9. $\mathbb{F}_9$
10. $\mathbb{F}_{10}$ No existe

6. Sean $n \geq 1$ y p un numero primo. Demostrad $\forall x \in \mathbb{F}_{p^n} \exists! y \in \mathbb{F}_{p^n} \mid y^p = x$.