ÁLGEBRA 3

Segundo cuatrimestre — 2019

Práctica 5: Cuerpos finitos y extensiones infinitas

1. Sea K un cuerpo finito. Caracterizar los grupos $(K,+)$ y $(K^{\times},\cdot)$, en términos del teorema de estructuras para grupos abelianos finitos.

2. Sea E una clausura algebraica de $\mathbb{F}_p$. Dados $m,n \in \mathbb{N}$, sean $\mathbb{F}_{p^m}, \mathbb{F}_{p^n} \subseteq E$ los cuerpos de p^m y p^n elementos. Probar que $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ si y solo si $m \mid n$.

3. Sea K un cuerpo finito. Probar que para todo $n \in \mathbb{N}$ existen polinomios irreducibles en $K[X]$ de grado n.

4. Sea K un cuerpo finito de q elementos. Para cada $n \geq 1$ denotemos por $u(n)$ a la cantidad de polinomios irreducibles mónicos de grado n en $K[X]$.

(a) Probar que $q^n = \sum_{d|n} d \cdot u(d)$.

$(b)^{\dagger}$ Dar una fórmula para $u(n)$.

5. Sea $f \in \mathbb{F}_q[X]$ irreducible de grado n y sea $k \in \mathbb{N}$. Probar que f se factoriza en $\mathbb{F}_{q^k}[X]$ como producto de polinomios irreducibles de grado $\frac{n}{d}$, donde $d = \gcd(n,k)$. Concluir que f sigue siendo irreducible en $\mathbb{F}_{q^k}[X]$ si y solo si n y k son coprimos.

6. Sea K un cuerpo finito, y sean E, L extensiones de K de grados m y n respectivamente.

(a) Probar que $[EL : K] = \mathsf{mcm}(m,n)$.

(b) Probar que $[E \cap L : K] = \mathsf{mcd}(m,n)$.

7. Sea E una clausura algebraica de $\mathbb{F}_p$ Sea $\sigma \in \mathsf{Gal}(E/\mathbb{F}_p)$ el automorfismo de Frobenius.

(a) Probar que σ tiene orden infinito.

(b) Probar que $\langle \sigma \rangle \subsetneq \mathsf{Gal}(E/\mathbb{F}_p)$.

8. Sea E/K una extensión galoisiana y sean H, H' subgrupos cerrados de $\mathsf{Gal}(E/K)$ tales que $H \leq H'$ y $[H' : H] < \infty$. Probar que la extensión $E^H/E^{H'}$ es finita, y $\left[E^H : E^{H'}\right] = [H' : H]$.

9. Sea E/K una extensión galoisiana, y sea S un subconjunto de $\mathsf{Gal}(E/K)$. Sea E^S la subextensión dada por

$$E^S = \{x \in E : \sigma x = x \quad \forall \sigma \in S\}.$$

Probar que $\mathsf{Gal}\left(E/E^S\right)$ es la clausura del subgrupo de $\mathsf{Gal}(E/K)$ generado por S.

10. Sea E/K una extensión galoisiana, y sea $\mathscr{F}$ una familia de subextensiones galoisianas de E/K tales que

- $E = \bigcup_{F \in \mathscr{F}} F$.
- Dadas $F, F' \in \mathscr{F}$, existe $F'' \in \mathscr{F}$ tal que $FF' \subseteq F''$.

Probar que

$$\mathsf{Gal}(E/K) \simeq \varprojlim_{F\in\mathscr{F}} \mathsf{Gal}(F/K).$$

11. Sea p un primo. Para cada $n \geq 1$ sea ξ_{p^n} una raíz primitiva p^n-ésima de la unidad, y sea $E/\mathbb{Q}$ la extensión galoisiana dada por

$$E = \mathbb{Q}\big(\{\xi_{p^n} : n \geq 1\}\big).$$

Probar que

$$\mathsf{Gal}(E/\mathbb{Q}) \simeq \varprojlim_{n\geq 1} (\mathbb{Z}/p^n\mathbb{Z})^\times.$$

12. Sea p un primo, y sea E una clausura algebraica de $\mathbb{F}_p$.

(a) Probar que

$$\mathsf{Gal}\big(E/\mathbb{F}_p\big) \simeq \varprojlim_{n\geq 1} \mathbb{Z}/n\mathbb{Z}.$$

(b) Sea $\sigma \in \mathsf{Gal}(E/\mathbb{F}_p)$ el automorfismo de Frobenius. Probar que

$$\mathsf{Gal}\big(E/\mathbb{F}_p\big) = \overline{\langle\sigma\rangle}.$$

(c) Para cada primo q, hallar una subextensión cuyo grupo de Galois sea isomorfo a $\mathbb{Z}_q$.

13‡ Probar que el único elemento no trivial de orden finito de $\mathsf{Gal}\big(\overline{\mathbb{Q}}/\mathbb{Q}\big)$ es la conjugación compleja.

Wolfgang Krull
1899–1971, Alemania