Università degli Studi Roma Tre
Corso di laurea in Matematica A.A. 2013-2014
AL310 - Istituzioni di Algebra Superiore
14 Novembre 2013 - Esercitazione n.4
Antonio Cigliola

Esercizio 1. Sia F un campo con 2^f elementi. Dimostrare che ogni elemento di F diverso da 0 e da 1 è un generatore di F^* se e solo se $2^f - 1$ è primo.

Esercizio 2. Determinare il campo di spezzamento K del polinomio

$$f(x) = x^5 + x^4 + 1 \in \mathbb{Z}_2[x].$$

Verificare che K è isomorfo al campo $\mathbb{F}_{64}$ esibendo concretamente un isomorfismo. Determinare esplicitamente $\mathfrak{Gal}_{\mathbb{F}_2}(K)$ e $\mathfrak{Gal}_{\mathbb{F}_2}(\mathbb{F}_{64})$ e stabilire se hanno la stessa struttura.

Esercizio 3. Trovare, se esistono, α e β tali che $\mathbb{F}_{16} \cong \mathbb{F}_2(\alpha, \beta)$. Calcolare esplicitamente $\mathfrak{Gal}_{\mathbb{F}_2}(\mathbb{F}_2(\alpha, \beta))$ estendendo gli $\mathbb{F}_2$-isomorfismi di $\mathbb{F}_2(\alpha)$. Stabilire se $\mathfrak{Gal}_{\mathbb{F}_2}(\mathbb{F}_2(\alpha, \beta))$ è un gruppo ciclico. In caso affermativo trovare tutti i suoi generatori.

Esercizio 4. Elencare tutti i polinomi monici irriducibili di grado 1, 2, 3, 4, 5 e 6 su $\mathbb{Z}_2$.

Esercizio 5. Sia F un campo. Provare che il polinomio $x^d - 1$ divide il polinomio $x^n - 1$ in $F[X]$ se e solo se $d \mid n$.

Esercizio 6. Siano p un numero primo e $k \geqslant 1$ un intero. Sia $F \subseteq K$ un'estensione di campi di grado p^k. Sia $f(x) \in F[x]$ un polinomio irriducibile su F di grado strettamente compreso tra 1 e p. Dimostrare che $f(x)$ non ha radici in K.

Esercizio 7. Provare che se d è un divisore positivo di n, il polinomio $x^{p^d} - x$ divide il polinomio $x^{p^n} - x$ in $\mathbb{Z}_p[x]$.

Esercizio 8. Provare che tutti e soli i sottocampi del campo $\mathbb{F}_{p^n}$ sono i campi $\mathbb{F}_{p^d}$ con d divisore positivo di n.

Esercizio 9. Costriure i campi con 2, 3, 4, 8, 9, 16, 25, 27, 32 e 64 elementi. Determinare per ciascuno di essi il gruppo di Galois (sul sottocampo fondamentale) e la sua struttura.

Esercizio 10. Trovare tutti i polinomi monici irriducibili di grado 1, 2, 3 e 4 su $\mathbb{Z}_3$.

Esercizio 11. Determinare esplicitamente i gruppi $\mathfrak{Gal}_{\mathbb{F}_2}(\mathbb{F}_{64})$, $\mathfrak{Gal}_{\mathbb{F}_4}(\mathbb{F}_{64})$, $\mathfrak{Gal}_{\mathbb{F}_8}(\mathbb{F}_{64})$, $\mathfrak{Gal}_{\mathbb{F}_4}(\mathbb{F}_{16})$ e le loro strutture.

Esercizio 12. Qual è la probabilità che un polinomio monico a coefficienti in $\mathbb{Z}_2$ di grado 5 abbia un fattore irriducibile di grado 2?