

ISTITUZIONI DI ALGEBRA SUPERIORE

Claudia Malvenuto
Scheda di esercizi n. 9

1. Cercare polinomi binari irriducibili di grado 2, 3 e 5.
2. Trovare un polinomio di grado 3 irriducibile su $GF(3)$. Fare qualche calcolo algebrico nel campo $GF(27)$.
3. Costruire esplicitamente $GF(8)$, $GF(9)$ e scrivere le loro tavole moltiplicative e additive.
4. Dato il polinomio $f(x) = \sum_{i=0}^n a_i x^i$, $a_i \in GF(p^m)$, la sua derivata è il polinomio

$$\frac{df(x)}{dx} = f'(x) = \sum_{i=1}^n i a_i x^{i-1}.$$

Dimostrare che se $(x - \alpha)^k$ divide $f(x)$, allora $(x - \alpha)^{k-1}$ divide $f'(x)$; che se $f(x)$ non ha zeri multipli in qualunque estensione, allora $f(x)$ e $f'(x)$ sono primi fra loro; che per $p = 2$, $f'(x)$ contiene solo potenze pari ed è un quadrato perfetto, inoltre $f''(x) = 0$.

5. Sia F una estensione finita di $GF(p)$ che contiene gli zeri del polinomio $x^{p^m} - 1$. Dimostrare che $x^{p^m} - 1$ ha tutti zeri distinti; mostrare direttamente che questi zeri formano un campo.
6. In un gruppo commutativo G , siano g ed h elementi di ordine rispettivamente r , s . Mostrare che se $g^n = 1$ allora $r|n$; che se r ed s sono coprimi allora gh ha ordine rs e che se $r = r'r''$ allora $g^{r'}$ ha ordine r'' .
7. Mostrare che l'applicazione $\gamma \mapsto \gamma^p$ è un isomorfismo di $GF(p^m)$ in sé.
8. Mostrare che in ogni campo:

$$x^s - 1 | x^r - 1 \Leftrightarrow s | r.$$

Mostrare inoltre che $\text{mcd}(x^r - 1, x^s - 1) = x^d - 1$, dove $d = \text{mcd}(r, s)$.

9. Trovare le classi ciclotomiche $\pmod{8}$ e $\pmod{26}$, con $p = 3$.
10. Sia $a(x) = a_0 + a_1x + \dots + a_{r-1}x^{r-1} + x^r$ un polinomio monico e $C(a)$ la matrice compagna ad esso associata:

$$C(a) = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ 0 & 0 & 0 & \dots & 1 \\ -a_0 & -a_1 & -a_2 & \dots & -a_{r-1} \end{bmatrix} :$$

dimostrare che il polinomio caratteristico di $C(a)$ è il polinomio $a(x)$ stesso.

11. Sapendo che sia il polinomio caratteristico $\det(C(a) - xI)$ che il polinomio minimo della matrice compagna $C(a)$ di un polinomio $a(x)$ sono il polinomio stesso, dimostrare che, fissato un polinomio monico $\pi(x) \in GF(p)[x]$ irriducibile su $GF(p)$ e di grado m , allora la matrice compagna $M = C(\pi)$ di ordine $m \times m$ del polinomio $\pi(x)$ è tale che:

- (a) $M^i = I$, se $i = p^m - 1$;
(b) $M^i \neq I$, se $1 \leq i < p^m - 1$;

pertanto M risulta essere un elemento primitivo per $GF(p^m)$, e questo fornisce una presentazione alternativa matriciale per il campo finito a p^m elementi.

12. Studiare la fattorizzazione in irriducibili di $x^{16} + x$ ed elencare i polinomi minimi degli elementi di $GF(16)$ scegliendo $\pi(x) = x^4 + x + 1$ come polinomio per costruire l'estensione $GF(16) \supset GF(2)$.
13. Studiare la fattorizzazione in irriducibili di $x^{25} + x$ ed elencare i polinomi minimi degli elementi di $GF(32)$ scegliendo $\pi(x) = x^5 + x + 1$ come polinomio per costruire l'estensione $GF(32) \supset GF(2)$.
14. Sia $f(x) \in GF(p)[x]$ un polinomio primo di fattori quadratici di grado $n > 0$. Dimostrare che:
- (a) se $\text{MCD}(f, x^{q^i} - x) = 1$ per $i = 1, 2, \dots, [n/2]$, allora f è irriducibile;
- (b) se f è un divisore di $x^{q^n} - x$ e $\text{MCD}(f, x^{q^{n/l}} - x) = 1$ per ogni primo l che divide n , allora f è irriducibile.