TRENTO, A.A. 2022/23
CORSO DI ALGEBRA B
FOGLIO DI ESERCIZI # 8

Esercizio 8.1. Sia $E \supseteq \mathbf{F}_p$ un campo di caratteristica il primo p.

Sia $f \in F_p[x]$ un polinomio di grado positivo.

Si mostri che se $\alpha \in E$ è un radice di f, allora lo sono anche $\alpha^p, \alpha^{p^2}, \dots, \alpha^{p^i}, \dots$.

Esercizio 8.2. Sia E un campo finito di ordine p^n, con p primo e $n > 0$ un intero.

Si assuma come noto che il gruppo moltiplicativo E^* sia ciclico.

Si mostri che esiste $\alpha \in E$ tale che

(1) $E = \mathbf{F}_p[\alpha]$, e
(2) il polinomio minimo di α su F_p è un polinomio irriducibile di grado n in $\mathbf{F}_p[x]$.

Esercizio 8.3. Si mostri che c'è un unico polinomio irriducibile f di grado 2 in $\mathbf{F}_2[x]$.

Si costruisca un campo $E = \mathbf{F}_2[\alpha]$ con 4 elementi, ove α è radice di f.

Si trovino in E tutte le radici di f, e i polinomi minimi su $\mathbf{F}_2$ di tutti gli elementi.

Esercizio 8.4. Si trovino i due polinomi irriducibili f_1, f_2 di grado 3 in $\mathbf{F}_2[x]$.

Si costruisca un campo $E = \mathbf{F}_2[\alpha]$ con 8 elementi, ove α è radice di f_1. Si calcolino le potenze di α, costruendo la tabella del logaritmo discreto. Si trovino in E tutte le radici di f_1 e f_2, e i polinomi minimi su $\mathbf{F}_2$ di tutti gli elementi.

Si costruisca un campo $E = \mathbf{F}_2[\beta]$ con 8 elementi, ove β è radice di f_2. Si calcolino le potenze di β, costruendo la tabella del logaritmo discreto. Si trovino in E tutte le radici di f_1 e f_2, e i polinomi minimi su $\mathbf{F}_2$ di tutti gli elementi.

Esercizio 8.5. Sia $\mathbf{F}_3 = \{ 0, 1, -1 \}$ il campo con 3 elementi.

Si trovino i tre polinomi monici e irriducibili f_1, f_2, f_3 di grado 2 in $\mathbf{F}_3[x]$, e sia $f_3 = x^2 + 1$.

Si costruisca un campo $E = \mathbf{F}_3[\alpha]$ con 9 elementi, ove α è radice di f_1. Si calcolino le potenze di α, costruendo la tabella del logaritmo discreto. Si trovino in E tutte le radici di f_1, f_2, f_3, e i polinomi minimi su $\mathbf{F}_3$ di tutti gli elementi.

Si costruisca un campo $E = \mathbf{F}_3[\beta]$ con 9 elementi, ove α è radice di f_2. Si calcolino le potenze di β, costruendo la tabella del logaritmo discreto. Si trovino in E tutte le radici di f_1, f_2, f_3, e i polinomi minimi su $\mathbf{F}_3$ di tutti gli elementi.

Esercizio 8.6. Si trovino i tre polinomi irriducibili f_1, f_2, f_3 di grado 4 in $\mathbf{F}_2[x]$, e sia $f_3 = x^4 + x^3 + x^2 + x + 1$.

Si costruisca un campo $E = \mathbf{F}_2[\alpha]$ con 16 elementi, ove α è radice di f_1. Si calcolino le potenze di α, costruendo la tabella del logaritmo discreto. Si trovino in E tutte le radici di f_1, f_2, f_3, e del polinomio f dell'esercizio 8.3.

Si costruisca un campo $E = \mathbf{F}_2[\beta]$ con 16 elementi, ove α è radice di f_2. Si calcolino le potenze di β, costruendo la tabella del logaritmo discreto. Si trovino in E tutte le radici di f_1, f_2, f_3, e del polinomio f dell'esercizio 8.3, e i polinomi minimi su $\mathbf{F}_2$ di tutti gli elementi.

Esercizio 8.7. Siano p un primo, e m, n interi positivi.

Si mostri che sono equivalenti

(1) un campo con p^n elementi contiene un campo con p^m elementi, e
(2) m divide n.

Esercizio 8.8. Definite la distanza di Hamming d su $\mathbf{F}_2^n$, e mostrate che soddisfa, per $a, b, c \in \mathbf{F}_2^n$,

(1) $d(a, b) = 0$ se e solo se $a = b$.
(2) $d(a, b) = d(b, a)$.
(3) $d(a, b) \leq d(a, c) + d(c, b)$.
(4) $d(a, b) = d(a - b, 0)$.

Esercizio 8.9. Sia $\mathcal{C}$ un codice lineare binario, e si definisca la sua distanza minima come

$$d(\mathcal{C}) = \min \{ d(a, b) : a, b \in \mathcal{C}, a \neq b \} .$$

Si mostri che

$$d(\mathcal{C}) = \min \{ d(a, 0) : a \in \mathcal{C}, a \neq 0 \} .$$

Esercizio 8.10 (Facoltativo). Sia $\mathcal{A} = \{ 0, 1, \dots, 10 \}$. Il codice ISBN-10 è il sottoinsieme $\mathcal{C}$ di $\mathcal{A}^{10}$, dato dai vettori $a = (a_1, a_2, \dots, a_{10})$ tali che $a_1, \dots, a_9 \in \{ 0, 1, \dots, 9 \}$, e l'ultima cifra a_{10} è calcolata mediante

$$a_{10} = \sum_{i=1}^{9} i \cdot a_i \pmod{11},$$

cioè a_{10} è il resto della divisione per 11 di $\sum_{i=1}^{9} i \cdot a_i$. (Se $a_{10} = 10$, sul retro dei libri si scrive `X`.) Notate anche che questa formula si può riscrivere nella forma

$$\sum_{i=1}^{10} i \cdot a_i \equiv 0 \pmod{11},$$

dato che $-1 \equiv 10 \pmod{11}$.

- Mostrare che $\mathcal{C}$ *rivela un errore*, nel senso che se $a \in \mathcal{C}$, e cambio *una* cifra di a, ottenendo un vettore b, allora $b \notin \mathcal{C}$
- Mostrare che $\mathcal{C}$ *rivela uno scambio*, nel senso che se $a \in \mathcal{C}$, e scambio due cifre *diverse* di a, ottenendo un vettore b, allora $b \notin \mathcal{C}$