QUARTA PROVETTA DI ALGEBRA
TRENTO, 18 DICEMBRE 2015

Nota: Questi fogli contengono gli esercizi delle quattro diverse versioni della provetta che sono state assegnate. L'esercizio $x.y$ è l'esercizio x della versione y.

Esercizio 1.1. Sia $n \geq 3$ un intero. Si consideri il gruppo delle permutazioni su $\Omega = \mathbf{Z}/n\mathbf{Z} = \{\, 0, 1, 2, \ldots, n-1 \,\}$

$$D_n = \{\, f_{a,b} : b \in \mathbf{Z}/n\mathbf{Z}, a \in \{\, 1, -1 \,\} \,\},$$

ove $f_{a,b} : x \mapsto ax + b$.

(1) Si mostri che $f_{1,1}$ ha periodo n.
(2) Si mostri che ogni $f_{-1,b}$ ha periodo 2, per $b \in \mathbf{Z}/n\mathbf{Z}$.
(3) Si mostri che D_n non è commutativo.
(4) Si calcoli $f_{-1,0} \circ f_{-1,-1}$ e se ne dica il periodo.

Esercizio 1.2. Sia $n \geq 3$ un intero. Si consideri il gruppo delle permutazioni su $\Omega = \mathbf{Z}/n\mathbf{Z} = \{\, 0, 1, 2, \ldots, n-1 \,\}$

$$D_n = \{\, f_{a,b} : b \in \mathbf{Z}/n\mathbf{Z}, a \in \{\, 1, -1 \,\} \,\},$$

ove $f_{a,b} : x \mapsto ax + b$.

(1) Si mostri che $f_{1,-1}$ ha periodo n.
(2) Si mostri che ogni $f_{-1,b}$ ha periodo 2, per $b \in \mathbf{Z}/n\mathbf{Z}$.
(3) Si mostri che D_n non è commutativo.
(4) Si calcoli $f_{-1,1} \circ f_{-1,0}$ e se ne dica il periodo.

Esercizio 1.3. Sia $n \geq 3$ un intero. Si consideri il gruppo delle permutazioni su $\Omega = \mathbf{Z}/n\mathbf{Z} = \{\, 0, 1, 2, \ldots, n-1 \,\}$

$$D_n = \{\, f_{a,b} : b \in \mathbf{Z}/n\mathbf{Z}, a \in \{\, 1, -1 \,\} \,\},$$

ove $f_{a,b} : x \mapsto ax + b$.

(1) Si mostri che $f_{1,1}$ ha periodo n.
(2) Si mostri che ogni $f_{-1,b}$ ha periodo 2, per $b \in \mathbf{Z}/n\mathbf{Z}$.
(3) Si mostri che D_n non è commutativo.
(4) Si calcoli $f_{-1,-1} \circ f_{-1,0}$ e se ne dica il periodo.

Esercizio 1.4. Sia $n \geq 3$ un intero. Si consideri il gruppo delle permutazioni su $\Omega = \mathbf{Z}/n\mathbf{Z} = \{\, 0, 1, 2, \ldots, n-1 \,\}$

$$D_n = \{\, f_{a,b} : b \in \mathbf{Z}/n\mathbf{Z}, a \in \{\, 1, -1 \,\} \,\},$$

ove $f_{a,b} : x \mapsto ax + b$.

(1) Si mostri che $f_{1,-1}$ ha periodo n.
(2) Si mostri che ogni $f_{-1,b}$ ha periodo 2, per $b \in \mathbf{Z}/n\mathbf{Z}$.
(3) Si mostri che D_n non è commutativo.

(4) Si calcoli $f_{-1,0} \circ f_{-1,1}$ e se ne dica il periodo.

Esercizio 2.1. Sia $V = F^n$ lo spazio delle n-ple sul campo $F = \mathbf{Z}/2\mathbf{Z}$. Per $a, b \in V$, si ponga la distanza (di Hamming) fra a e b pari a

$$d(a, b) = |\{ i : a_i \neq b_i \}|$$

(Sto usando la solita convenzione che $a = [a_0, a_1, \ldots, a_{n-1}]$, cioè che la componente i-sima di un vettore a è a_i.)

Si mostri che per $a, b, c \in V$.

$$d(a, b) \leq d(a, c) + d(c, b).$$

Esercizio 2.2. Sia $V = F^n$ lo spazio delle n-ple sul campo $F = \mathbf{Z}/2\mathbf{Z}$. Per $a, b \in V$, si ponga la distanza (di Hamming) fra a e b pari a

$$d(a, b) = |\{ i : a_i \neq b_i \}|$$

(Sto usando la solita convenzione che $a = [a_0, a_1, \ldots, a_{n-1}]$, cioè che la componente i-sima di un vettore a è a_i.)

Si mostri che per $a, b, c \in V$.

$$d(a, b) \leq d(a, c) + d(c, b).$$

Esercizio 2.3. Sia $V = F^n$ lo spazio delle n-ple sul campo $F = \mathbf{Z}/2\mathbf{Z}$. Per $a, b \in V$, si ponga la distanza (di Hamming) fra a e b pari a

$$d(a, b) = |\{ i : a_i \neq b_i \}|$$

(Sto usando la solita convenzione che $a = [a_0, a_1, \ldots, a_{n-1}]$, cioè che la componente i-sima di un vettore a è a_i.)

Si mostri che per $a, b, c \in V$.

$$d(a, b) \leq d(a, c) + d(c, b).$$

Esercizio 2.4. Sia $V = F^n$ lo spazio delle n-ple sul campo $F = \mathbf{Z}/2\mathbf{Z}$. Per $a, b \in V$, si ponga la distanza (di Hamming) fra a e b pari a

$$d(a, b) = |\{ i : a_i \neq b_i \}|$$

(Sto usando la solita convenzione che $a = [a_0, a_1, \ldots, a_{n-1}]$, cioè che la componente i-sima di un vettore a è a_i.)

Si mostri che per $a, b, c \in V$.

$$d(a, b) \leq d(a, c) + d(c, b).$$

Esercizio 3.1. Sia $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z} = \{ 0, 1 \}$ il campo con due elementi.

(1) Mostrate che il polinomio

$$f = x^3 + x^2 + 1 \in \mathbf{F}_2[x]$$

è irriducibile in $\mathbf{F}_2[x]$.

(2) Sia α una radice di f. Costruite la tabellina del logaritmo discreto nel campo $F[\alpha]$, ovvero calcolate le potenze di α come combinazioni lineari di $1, \alpha, \alpha^2$.

(3) Costruite una matrice di controllo di parità e una matrice del codice di Hamming che ha per parametro f.

(4) Codificate

$$[1, 1, 0, 1],$$
$$[1, 0, 1, 1],$$

e decodificate

$$[1, 0, 0, 1, 0, 1, 1],$$
$$[1, 0, 1, 0, 0, 1, 1].$$

Dunque per codificare occorre far vedere come fa il mittente ad associare ad un vettore di $\mathbf{F}_2^4$ (che contiene i *bit di informazione*) una parola del codice, che è un elemento di $\mathbf{F}_2^7$, aggiungendo quindi i *bit di controllo*. E per decodificare occorre far vedere come fa il ricevente a decidere se i vettori ricevuti sono parole del codice o no, e a ricostruire in ogni caso cosa ha trasmesso il mittente, assumendo che ci sia stato al più un errore.

Esercizio 3.2. Sia $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z} = \{ 0, 1 \}$ il campo con due elementi.

(1) Mostrate che il polinomio

$$f = x^3 + x + 1 \in \mathbf{F}_2[x]$$

è irriducibile in $\mathbf{F}_2[x]$.

(2) Sia α una radice di f. Costruite la tabellina del logaritmo discreto nel campo $F[\alpha]$, ovvero calcolate le potenze di α come combinazioni lineari di $1, \alpha, \alpha^2$.

(3) Costruite una matrice di controllo di parità e una matrice del codice di Hamming che ha per parametro f.

(4) Codificate

$$[1, 1, 0, 1],$$
$$[1, 0, 1, 1],$$

e decodificate

$$[1, 0, 0, 1, 0, 1, 1],$$
$$[1, 0, 1, 0, 0, 1, 1].$$

Dunque per codificare occorre far vedere come fa il mittente ad associare ad un vettore di $\mathbf{F}_2^4$ (che contiene i *bit di informazione*) una parola del codice, che è un elemento di $\mathbf{F}_2^7$, aggiungendo quindi i *bit di controllo*. E per decodificare occorre far vedere come fa il ricevente a decidere se i vettori ricevuti sono parole del codice o no, e a ricostruire in ogni caso cosa ha trasmesso il mittente, assumendo che ci sia stato al più un errore.

Esercizio 3.3. Sia $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z} = \{ 0, 1 \}$ il campo con due elementi.

(1) Mostrate che il polinomio

$$f = x^3 + x^2 + 1 \in \mathbf{F}_2[x]$$

è irriducibile in $\mathbf{F}_2[x]$.

(2) Sia α una radice di f. Costruite la tabellina del logaritmo discreto nel campo $F[\alpha]$, ovvero calcolate le potenze di α come combinazioni lineari di $1, \alpha, \alpha^2$.
(3) Costruite una matrice di controllo di parità e una matrice del codice di Hamming che ha per parametro f.
(4) Codificate

$$[0,1,1,1],$$
$$[1,1,1,0],$$

e decodificate

$$[0,1,0,1,1,1,0],$$
$$[1,1,0,1,0,0,1].$$

Dunque per codificare occorre far vedere come fa il mittente ad associare ad un vettore di $\mathbf{F}_2^4$ (che contiene i *bit di informazione*) una parola del codice, che è un elemento di $\mathbf{F}_2^7$, aggiungendo quindi i *bit di controllo*. E per decodificare occorre far vedere come fa il ricevente a decidere se i vettori ricevuti sono parole del codice o no, e a ricostruire in ogni caso cosa ha trasmesso il mittente, assumendo che ci sia stato al più un errore.

Esercizio 3.4. Sia $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z} = \{0, 1\}$ il campo con due elementi.

(1) Mostrate che il polinomio

$$f = x^3 + x + 1 \in \mathbf{F}_2[x]$$

è irriducibile in $\mathbf{F}_2[x]$.
(2) Sia α una radice di f. Costruite la tabellina del logaritmo discreto nel campo $F[\alpha]$, ovvero calcolate le potenze di α come combinazioni lineari di $1, \alpha, \alpha^2$.
(3) Costruite una matrice di controllo di parità e una matrice del codice di Hamming che ha per parametro f.
(4) Codificate

$$[0,1,1,1],$$
$$[1,1,1,0],$$

e decodificate

$$[0,1,0,1,1,1,0],$$
$$[1,1,0,1,0,0,1].$$

Dunque per codificare occorre far vedere come fa il mittente ad associare ad un vettore di $\mathbf{F}_2^4$ (che contiene i *bit di informazione*) una parola del codice, che è un elemento di $\mathbf{F}_2^7$, aggiungendo quindi i *bit di controllo*. E per decodificare occorre far vedere come fa il ricevente a decidere se i vettori ricevuti sono parole del codice o no, e a ricostruire in ogni caso cosa ha trasmesso il mittente, assumendo che ci sia stato al più un errore.

Esercizio 4.1. Sia G un gruppo, e sia H un sottogruppo di G. Si consideri la relazione su G data da

$$aTb \quad \text{se e solo se} \quad ab^{-1} \in H.$$

(1) Si mostri che T è una relazione di equivalenza.
(2) Per $a \in G$, si dica chi è la sua classe di equivalenza.

Esercizio 4.2. Sia G un gruppo, e sia H un sottogruppo di G. Si consideri la relazione su G data da

$$aTb \quad \text{se e solo se} \quad a^{-1}b \in H.$$

(1) Si mostri che T è una relazione di equivalenza.
(2) Per $a \in G$, si dica chi è la sua classe di equivalenza.

Esercizio 4.3. Sia G un gruppo, e sia H un sottogruppo di G. Si consideri la relazione su G data da

$$aTb \quad \text{se e solo se} \quad b^{-1}a \in H.$$

(1) Si mostri che T è una relazione di equivalenza.
(2) Per $a \in G$, si dica chi è la sua classe di equivalenza.

Esercizio 4.4. Sia G un gruppo, e sia H un sottogruppo di G. Si consideri la relazione su G data da

$$aTb \quad \text{se e solo se} \quad ba^{-1} \in H.$$

(1) Si mostri che T è una relazione di equivalenza.
(2) Per $a \in G$, si dica chi è la sua classe di equivalenza.

Esercizio 5.1. Si enunci e si dimostri il Secondo Teorema di Isomorfismo per gruppi.

Esercizio 5.2. Sia $G = \langle\, a \,\rangle$ un gruppo ciclico di ordine n.
Si mostri che G ha uno e un solo sottogruppo di ordine m, per ogni divisore m di n.

Esercizio 5.3. Si enunci e si dimostri il Secondo Teorema di Isomorfismo per gruppi.

Esercizio 5.4. Sia $G = \langle\, a \,\rangle$ un gruppo ciclico di ordine n.
Si mostri che G ha uno e un solo sottogruppo di ordine m, per ogni divisore m di n.

Esercizio 6.1. Si enunci il Terzo Teorema di Isomorfismo per gruppi.

Esercizio 6.2. Si enunci il Terzo Teorema di Isomorfismo per anelli.

Esercizio 6.3. Si enunci il Terzo Teorema di Isomorfismo per gruppi.

Esercizio 6.4. Si enunci il Terzo Teorema di Isomorfismo per anelli.

Esercizio 7.1. Siano A, B insiemi, $f : A \to B$ una funzione.

(1) Per $L \subseteq A$, si definisca $f(L)$.
(2) Per $N \subseteq B$, si definisca $f^{-1}(N)$.
(3) Per $L, M \subseteq A$, si mostri che $f(L \cap M) \subseteq f(L) \cap f(M)$. Si mostri con un esempio che non sempre vale l'eguaglianza.

(4) Per $N, P \subseteq B$, si mostri che $f^{-1}(N \cap P) = f^{-1}(N) \cap f^{-1}(P)$.

Esercizio 7.2. Siano A, B insiemi, $f : A \to B$ una funzione.

(1) Per $L \subseteq A$, si definisca $f(L)$.
(2) Per $N \subseteq B$, si definisca $f^{-1}(N)$.
(3) Per $L, M \subseteq A$, si mostri che $f(L \cap M) \subseteq f(L) \cap f(M)$. Si mostri con un esempio che non sempre vale l'eguaglianza.
(4) Per $N, P \subseteq B$, si mostri che $f^{-1}(N \cup P) = f^{-1}(N) \cup f^{-1}(P)$.

Esercizio 7.3. Siano A, B insiemi, $f : A \to B$ una funzione.

(1) Per $L \subseteq A$, si definisca $f(L)$.
(2) Per $N \subseteq B$, si definisca $f^{-1}(N)$.
(3) Per $L, M \subseteq A$, si mostri che $f(L \cap M) \subseteq f(L) \cap f(M)$. Si mostri con un esempio che non sempre vale l'eguaglianza.
(4) Per $N, P \subseteq B$, si mostri che $f^{-1}(N \cap P) = f^{-1}(N) \cap f^{-1}(P)$.

Esercizio 7.4. Siano A, B insiemi, $f : A \to B$ una funzione.

(1) Per $L \subseteq A$, si definisca $f(L)$.
(2) Per $N \subseteq B$, si definisca $f^{-1}(N)$.
(3) Per $L, M \subseteq A$, si mostri che $f(L \cap M) \subseteq f(L) \cap f(M)$. Si mostri con un esempio che non sempre vale l'eguaglianza.
(4) Per $N, P \subseteq B$, si mostri che $f^{-1}(N \cup P) = f^{-1}(N) \cup f^{-1}(P)$.

Esercizio 8.1. Se $0 \neq a \in \mathbf{Z}[x]$,

$$a = a_0 + a_1 x + \cdots + a_n x^n,$$

si dice che a è *primitivo* se

$$\gcd(a_0, a_1, \ldots, a_n) = 1.$$

Si mostri che il prodotto di polinomi primitivi è primitivo.

Esercizio 8.2. Se $0 \neq a \in \mathbf{Z}[x]$,

$$a = a_0 + a_1 x + \cdots + a_n x^n,$$

si dice che a è *primitivo* se

$$\gcd(a_0, a_1, \ldots, a_n) = 1.$$

Si mostri che il prodotto di polinomi primitivi è primitivo.

Esercizio 8.3. Se $0 \neq a \in \mathbf{Z}[x]$,

$$a = a_0 + a_1 x + \cdots + a_n x^n,$$

si dice che a è *primitivo* se

$$\gcd(a_0, a_1, \ldots, a_n) = 1.$$

Si mostri che il prodotto di polinomi primitivi è primitivo.

Esercizio 8.4. Se $0 \neq a \in \mathbf{Z}[x]$,

$$a = a_0 + a_1 x + \cdots + a_n x^n,$$

si dice che a è *primitivo* se

$$\gcd(a_0, a_1, \ldots, a_n) = 1.$$

Si mostri che il prodotto di polinomi primitivi è primitivo.