TRENTO, A.A. 2015/16
CORSO DI ALGEBRA
FOGLIO DI ESERCIZI # 12

Esercizio 12.1.

(1) Si costruisca il codice di Hamming sul campo con 8 elementi, usando prima uno poi l'altro dei due polinomi irriducibili di grado 3 su $\mathbf{F}_2$.
(2) Si mostri che entrambi i codici sono sottospazi di dimensione 4 di $\mathbf{F}_2^7$.
(3) Per entrambi i codici, si costruiscano le matrici H e C.
(4) Si mostri che entrambi i codici correggono un errore.
(5) Si mostri che entrambi sono codici ciclici, nel senso che se un codice contiene

$$[a_6, a_5, \ldots, a_1, a_0],$$

allora contiene

$$[a_5, \ldots, a_1, a_0, a_6].$$

(6) Si elenchino (meglio in maniera ragionata) gli elementi dei due codici.
(7) Si mostri come avviene la codifica, e si dia un paio di esempi di decodifica.
(8) Che legame c'è fra i due codici ottenuti?

Esercizio 12.2.

(1) Si costruisca il codice di Hamming sul campo con 16 elementi, usando prima uno poi l'altro dei due polinomi irriducibili di grado 4 su $\mathbf{F}_2$. (Dunque i polinomi sono $x^4 + x + 1$ e $x^4 + x^3 + 1$.)
(2) Si mostri che entrambi i codici sono sottospazi di dimensione 11 di $\mathbf{F}_2^{15}$.
(3) Per entrambi i codici, si costruiscano le matrici H e C.
(4) Si mostri che entrambi i codici correggono un errore.
(5) Si mostri che entrambi sono codici ciclici, nel senso che se un codice contiene

$$[a_{14}, a_{13}, \ldots, a_1, a_0],$$

allora contiene

$$[a_{13}, \ldots, a_1, a_0, a_{14}].$$

(6) Si mostri come avviene la codifica, e si dia un paio di esempi di decodifica.
(7) Che legame c'è fra i due codici ottenuti?

Esercizio 12.3. Chi è il codice di Hamming sul campo con 4 elementi, ovvero quello basato sull'unico polinomio irriducibile di grado 2 in $\mathbf{F}_2[x]$?

Esercizio 12.4. Per tutti i codici precedenti, si descriva la codifica mediante la divisione di polinomi, esibendo un esempio.

Esercizio 12.5. Sia $\Omega = \mathbf{Z}/n\mathbf{Z} = \{\, 0, 1, \ldots, n-1 \,\}$.

(1) Per $a, b \in \mathbf{Z}/n\mathbf{Z}$, si definisca la $f_{a,b}$ su Ω data da

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

(2) Si mostri che $f_{a,b} = f_{c,d}$ se e solo se $a = c$ e $b = d$.
(3) Si mostri che $f_{1,0}$ è la funzione identica su Ω.

(4) Si mostri che l'insieme
$$N = \{ f_{a,b} : a, b \in \mathbf{Z}/n\mathbf{Z} \}$$
è un monoide rispetto alla composizione.
(5) Si mostri che $f_{a,b}$ è invertibile in N se e solo se a è invertibile, e in tal caso
$$f_{a,b}^{-1} = f_{a^{-1},-a^{-1}b}.$$
(6) Si mostri che
$$N = \{ f_{a,b} : a \in U(\mathbf{Z}/n\mathbf{Z}), b \in \mathbf{Z}/n\mathbf{Z} \}$$
è un gruppo rispetto alla composizione, di ordine $n \cdot \varphi(n)$, ove φ è la funzione di Eulero.

Esercizio 12.6. Sia $n \geq 3$. Con le notazioni dell'esercizio precedente, si consideri l'insieme
$$D_n = \{ f_{\varepsilon,b} : \varepsilon \in \{ 1, -1 \}, b \in \mathbf{Z}/n\mathbf{Z} \}.$$
(1) Si mostri che D_n è un gruppo rispetto alla composizione, di ordine $2n$, detto il *gruppo diedrale*. (Ahimè, parecchi autori scrivono D_{2n} per lo stesso gruppo, dunque quando trovate il gruppo diedrale su qualche testo, accertatevi quale sia la notazione usata.)
(2) Si mostri che $f_{1,1}^k = f_{1,k}$.
(3) Si mostri che l'elemento $f_{1,1}$ ha periodo n, e dunque
$$\langle f_{1,1} \rangle$$
è un gruppo di ordine n, e che i suoi elementi sono
$$1, f_{1,1}, f_{1,2}, \ldots, f_{1,n-1}.$$
(4) Si trovi il periodo di ogni $f_{1,b}$, per $b \in \mathbf{Z}/n\mathbf{Z}$.
(5) Si mostri che ogni elemento $f_{-1,b}$, per $b \in \mathbf{Z}/n\mathbf{Z}$, ha periodo 2.
(6) Si mostri che
$$f_{-1,1} \circ f_{-1,0} = f_{1,1}$$
(con la composizione fatta da destra a sinistra), dunque il prodotto di due elementi di periodo 2 può avere periodo n arbitrario.
(7) Si mostri che
$$f_{-1,0} \circ f_{-1,1} = f_{1,-1}.$$

Esercizio 12.7. Sia G un gruppo, e N un suo sottogruppo. Si mostri che sono equivalenti
(1) Per ogni $a \in G$ si ha $Na = aN$.
(2) Per ogni $a \in G$ esiste $b \in G$ tale che $Na = bN$.
(3) Per ogni $a \in G$ si ha $a^{-1}Na \subseteq N$.
(4) Per ogni $a \in G$ si ha $a^{-1}Na = N$.

Esercizio 12.8. Siano G, H gruppi, e $f : G \to H$ un morfismo suriettivo.
(1) Si mostri che $N = \ker(f) = \{ a \in G : f(a) = 1 \}$ è un sottogruppo normale di G.

(2) Posta R la relazione (che abbiamo visto essere di equivalenza) su G data da aRb se e solo se $f(a) = f(b)$, si mostri che aRb se e solo se $a^{-1}b \in N$ se e solo se $aN = bN$. Se ne deduca che detta $[a] = \{ x \in G : aRx \}$ la classe di equivalenza di $a \in G$ rispetto a R, allora $[a] = aN$.
(3) Viceversa, se N è un sottogruppo normale del gruppo G, si mostri che la relazione R su G data da aRb se e solo se $a^{-1}b \in N$ è una relazione di equivalenza compatibile con le operazioni.
(4) Se ne deduca che posto $G/N = \{ aN : a \in G \}$, l'operazione $aN \cdot bN = (ab)N$ su G/N è ben definita, e che con questa operazione G/N diventa un gruppo.
(5) Si mostri che $\pi : G \to G/N$ dato da $a \mapsto aN$ è un morfismo suriettivo.

Esercizio 12.9. Si enunci e si dimostri il primo teorema di isomorfismo per i gruppi, nella seconda forma con i sottogruppi normali.

Esercizio 12.10. Si enunci e si dimostri il secondo teorema di isomorfismo per i gruppi.

In particolare, si mostri che se G è un gruppo, H è un sottogruppo, e N è un sottogruppo normale, allora $HN = \{ hn : h \in H, n \in N \}$ è un sottogruppo di G.

Esercizio 12.11. Si mostri che un morfismo di gruppi è iniettivo se e solo se il nucleo consiste del solo elemento neutro.

Esercizio 12.12. Si enunci il secondo teorema di isomorfismo per gli anelli.

Esercizio 12.13. Si consideri il gruppo diedrale $G = D_3$ di ordine 6.

Si considerino i sottogruppi di G

$$H = \langle f_{-1,0} \rangle, \qquad K = \langle f_{-1,1} \rangle.$$

Si mostri che

(1) H e K hanno ordine 2,
(2) HK ha ordine 4, e
(3) HK non è un sottogruppo di G.