TRENTO, A.A. 2020/21
CORSO DI ALGEBRA B
FOGLIO DI ESERCIZI # 11

Esercizio 11.1. 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 $\mathbf{F}_2$.

Si mostri come avviene la codifica, e si dia un paio di esempi di codifica e di decodifica.

Si mostri che questi codici sono ciclici, nel senso che se $\mathcal{C}$ è uno di essi, allora

$$[a_6, a_5, a_4, a_3, a_2, a_1, a_0] \in \mathcal{C} \quad \text{implica} \quad [a_5, a_4, a_3, a_2, a_1, a_0, a_6] \in \mathcal{C}.$$

Che legame c'è fra i due codici ottenuti?

Esercizio 11.2 (Questo è del tutto opzionale). Si costruisca il codice di Hamming sul campo con 16 elementi, usando prima l'uno e poi l'altro dei due polinomi irriducibili primitivi di grado 4 su $\mathbf{F}_2$. (Dunque i polinomi sono $x^4 + x + 1$ e $x^4 + x^3 + 1$.)

Si mostri come avviene la codifica, e si dia un paio di esempi di decodifica.

Esercizio 11.3. Si mostri che il codice di Hamming sul campo con 4 elementi, ovvero quello basato sull'unico polinomio irriducibile di grado 2 in $\mathbf{F}_2[x]$ (ovvero su un elemento α tale che $\alpha^2 + \alpha + 1$) è il codice a ripetizione 3 volte.

Esercizio 11.4. Si dia una descrizione sommaria del codice di Hamming basato su un polinomio irriducibile e primitivo di grado n in $\mathbf{F}_2[x]$.

Esercizio 11.5. Sia G un gruppo,e $H, K \leq G$. Sia

$$HK = \{\, hk : h \in H, k \in K \,\}.$$

(1) Si mostri con un esempio che in generale HK non è un sottogruppo di G.
(2) Si mostri che se $K \trianglelefteq G$, allora HK è un sottogruppo di G.

Esercizio 11.6. Enunciate e dimostrate il

Teorema (Secondo teorema di isomorfismo per gruppi). *Sia G un gruppo, H un suo sottogruppo, N un suo sottogruppo normale.*

(1) $HN = \{\, xy : x \in H, y \in N \,\}$ è un sottogruppo di G contenente il sottogruppo normale N.
(2) $H \cap N$ è un sottogruppo normale di H.
(3) La funzione

$$\psi : \frac{H}{H \cap N} \to \frac{HN}{N}$$
$$xH \cap N \mapsto xN$$

è un isomorfismo di gruppi.

Esercizio 11.7. Siano A, B insiemi, $f : A \to B$ una funzione.

Si ricordi che

(i) per $M \subseteq A$ si definisce
$$f(M) = \{\, f(x) : x \in M \,\};$$
(ii) per $L \subseteq B$ si definisce
$$f^{-1}(L) = \{\, x \in A : f(x) \in L \,\}.$$

Si mostri che

(1) per $L \subseteq B$ si ha
$$f(f^{-1}(L)) = L \cap f(A);$$
(2) per $M \subseteq A$ si ha
   (a)
   $$f^{-1}(f(M)) = \{\, x \in A : f(x) = f(a) \text{ per qualche } a \in M \,\};$$
   (b)
   $$f(f^{-1}(f(M))) = f(M).$$

Esercizio 11.8. Enunciate e dimostrate il

Teorema (Terzo teorema di isomorfismo per gruppi). *Sia G un gruppo, N un suo sottogruppo normale, $\pi : G \to G/N$ il morfismo canonico.*

(1) I sottogruppi di G/N si scrivono in modo unico nella forma H/N, ove H è un sottogruppo di G che contiene N;
(2) se $K \leq G$, allora $\pi(K) = KN/N$;
(3) sia H un sottogruppo di G che contiene N, allora H/N è normale in G/N se e solo se H è normale in G;
(4) se H è un sottogruppo normale di G che contiene N, si ha un isomorfismo fra
$$\frac{G/N}{H/N} \qquad e \qquad G/H.$$

Esercizio 11.9. Siano $a, b, m, n > 0$ interi.

(1) Si mostri che $a\mathbf{Z} \cap b\mathbf{Z} = \operatorname{lcm}(a, b)\mathbf{Z}$.
(2) Si mostri che $a\mathbf{Z} + b\mathbf{Z} = \gcd(a, b)\mathbf{Z}$.
(3) Si mostri che $m\mathbf{Z} \supseteq n\mathbf{Z}$ se e solo se $m \mid n$, e che in tal caso
$$\left| \frac{m\mathbf{Z}}{n\mathbf{Z}} \right| = \frac{n}{m}.$$
(4) Si usi il secondo teorema di isomorfismo per gruppi per mostrare che
$$\frac{a\mathbf{Z}}{\operatorname{lcm}(a, b)\mathbf{Z}} \cong \frac{\gcd(a, b)\mathbf{Z}}{b\mathbf{Z}}.$$
(5) Se ne deduca la formula
$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = a \cdot b.$$