TRENTO, A.A. 2022/23
CORSO DI ALGEBRA B
FOGLIO DI ESERCIZI # 10

Esercizio 10.1. 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 10.2. 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 10.3. 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 10.4. 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 10.5. 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 10.6. Siano $a, b, m, n > 0$ interi.

(1) Si mostri che $a\mathbf{Z} \cap b\mathbf{Z} = \mathrm{lcm}(a, b)\mathbf{Z}$.
(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

$$\frac{a\mathbf{Z}}{\mathrm{lcm}(a, b)\mathbf{Z}} \cong \frac{\gcd(a, b)\mathbf{Z}}{b\mathbf{Z}}.$$

(5) Se ne deduca la formula

$$\gcd(a, b) \cdot \mathrm{lcm}(a, b) = a \cdot b.$$

Esercizio 10.7. Ricordando che se $G = \langle\, a \,\rangle$ è un gruppo ciclico di ordine n, allora c'è un isomorfismo

$$\begin{aligned} \varphi : \mathbf{Z}/n\mathbf{Z} &\to G \\ [k] &\mapsto a^k, \end{aligned}$$

si mostri, usando i teoremi di isomorfismo, che un gruppo ciclico ha uno e un solo sottogruppo per ogni divisore dell'ordine.

Esercizio 10.8. Enunciate e dimostrate il

Teorema (Secondo teorema di isomorfismo per anelli). *Sia A un anello, B un suo sottoanello, I un suo ideale.*

(1) $B + I = \{\, x + y : x \in B, y \in I \,\}$ è un sottoanello di A contenente l'ideale I.
(2) $B \cap I$ è un ideale di B.
(3) La funzione

$$\begin{aligned} \psi : \frac{B}{B \cap I} &\to \frac{B + I}{I} \\ x + B \cap I &\mapsto x + I \end{aligned}$$

è un isomorfismo di anelli.

Esercizio 10.9. Si enunci e si dimostri il

Teorema (Terzo teorema di isomorfismo per anelli). *Sia A un anello, I un suo ideale*

(1) I sottoanelli di A/I sono della forma J/I, ove J è un sottoanello di A che contiene I;
(2) sia J un sottoanello di A contenente I, allora J/I è un ideale di A/I se e solo se J è un ideale di A;
(3) se J è un ideale di A contenente I, si ha un isomorfismo fra

$$\frac{A/I}{J/I} \qquad e \qquad A/J.$$

Esercizio 10.10. Si trovi in $\mathbf{Z}$ un esempio di due sottogruppi (che sono dunque anche sottoanelli e ideali) tali che la loro unione non sia un sottogruppo (e dunque neanche un sottoanello o un ideale.

(Suggerimento: Prendete ad esempio $2\mathbf{Z}$ e $3\mathbf{Z}$.)

Esercizio 10.11.

(1) Sia G un gruppo, $H, K \leq G$.
Si mostri che sono equivalenti:
  (a) $H \cup K$ è un sottogruppo di G, e
  (b) $H \subseteq K$ o $K \subseteq H$.
  (Suggerimento: Si supponga $H \not\subseteq K$, e si mostri che $K \subseteq H$.)
(2) Si enuncino e si dimostrino le affermazioni analoghe per sottoanelli e ideali.
(3) Mostrate che l'unione di una successione ascendente

$$X_1 \subseteq X_2 \subseteq \cdots \subseteq X_n \subseteq \dots$$

di sottogruppi/sottoanelli/ideali è un sottogruppo/sottoanello/ideale.