TRENTO, A.A. 2019/20
CORSO DI ALGEBRA A
FOGLIO DI ESERCIZI # 7

Esercizio 7.1.

(1) Mostrate che ogni relazione di equivalenza R su un insieme A è della forma, per $x, y \in A$,
$$xRy \iff f(x) = f(y)$$
per una opportuna funzione $f : A \to B$ da A a un opportuno insieme B.

(2) Mostrate che ogni relazione di equivalenza R su un gruppo G, tale che l'operazione $[x] \cdot [y] = [x \cdot y]$ fra le classi sia ben definita, è della forma, per $x, y \in G$,
$$xRy \iff f(x) = f(y)$$
per un opportuno morfismo $f : G \to H$ da G a un opportuno gruppo H.

(3) Mostrate che ogni relazione di equivalenza R su un anello A, tale che le operazioni $[x]+[y] = [x+y]$ e $[x]\cdot[y] = [x\cdot y]$ fra le classi siano ben definite, è della forma, per $x, y \in A$,
$$xRy \iff f(x) = f(y)$$
per un opportuno morfismo $f : A \to B$ da A a un opportuno anello B.

Esercizio 7.2.

(1) Definite le potenze (in un gruppo con notazione moltiplicativa) e i multipli (in un gruppo con notazione additiva).

(2) Enunciate e dimostrate (almeno la singola dimostrazione che ho fatto a lezione) le regole delle potenze.

(3) Mostrate con un esempio che se G è un gruppo, $n \in \mathbf{Z}$, in generale non vale $(ab)^n = a^n b^n$ per ogni $a, b \in G$.

(4) Sia G un gruppo, $a \in G$. Mostrate che la funzione
$$\begin{aligned} f : \mathbf{Z} &\to G \\ x &\mapsto a^x \end{aligned}$$
è un morfismo dal gruppo $(\mathbf{Z}, +, 0)$ a G, di immagine
$$\langle\, a \,\rangle = \{\, a^x : x \in \mathbf{Z} \,\}.$$

(5) Mostrate che se f è una funzione iniettiva, allora
$$\begin{aligned} f : \mathbf{Z} &\to \langle\, a \,\rangle \\ x &\mapsto a^x \end{aligned}$$
è un isomorfismo.

Esercizio 7.3. Sia G un gruppo, $a \in G$ e f il morfismo suriettivo
$$\begin{aligned} f : \mathbf{Z} &\to \langle\, a \,\rangle \\ x &\mapsto a^x \end{aligned}$$

(1) Mostrate che se f *non* è iniettivo, allora l'insieme

$$A = \{\, n \in \mathbf{N} : n > 0 \text{ e } a^n = 1 \,\} \subseteq \mathbf{N}$$

è non vuoto.

(2) Mostrate che A ha un minimo m.

(3) Mostrate che m è caratterizzato da queste due proprietà.
   (a) $m > 0$ e $a^m = 1$, e
   (b) se $n > 0$ e $a^n = 1$, allora $m \le n$.

   Questo m si dice *periodo* o *ordine* di a.

(4) Mostrate che si ha

$$\begin{cases} a^x = 1 & \text{se e solo se } m \mid x \\ a^x = a^y & \text{se e solo se } x \equiv y \pmod{m} \end{cases}$$

(5) Applicate il primo teorema di isomorfismo per gruppi per ottenere che la funzione

$$\begin{aligned} \varphi : \mathbf{Z}/m\mathbf{Z} &\to \langle\, a \,\rangle \\ [x] &\mapsto a^x \end{aligned}$$

è un isomorfismo.

(6) Mostrate che $\langle\, a \,\rangle$ è il più piccolo sottogruppo di G che contenga a.

(7) Mostrate che $\langle\, a \,\rangle$ ha m elementi, che sono

$$a^0 = 1, a^1 = a, a^2, \dots, a^{m-1}.$$

(8) Trovate il periodo di $[10]$ in $U(\mathbf{Z}/7\mathbf{Z})$ e in $U(\mathbf{Z}/11\mathbf{Z})$, e calcolatene tutte le potenze (distinte).