TRENTO, A.A. 2021/22
CORSO DI ALGEBRA A
FOGLIO DI ESERCIZI # 9

Esercizio 9.1. Sia G un gruppo, $a \in G$.

(1) Si mostri che la funzione
$$\begin{aligned} f : \mathbf{Z} &\to G \\ x &\mapsto a^x \end{aligned}$$
è un morfismo di gruppi.
(2) Si mostri che $\langle a \rangle = f(\mathbf{Z}) = \{ a^x : x \in \mathbf{Z} \}$ è un sottogruppo di G.
(3) Si mostri che $\langle a \rangle$ è il più piccolo sottogruppo di G che contenga a.
(4) D'ora in poi, si consideri il morfismo suriettivo
$$\begin{aligned} f : \mathbf{Z} &\to \langle a \rangle \\ x &\mapsto a^x \end{aligned}$$
(5) Mostrate che se f è iniettiva, ovvero $x \neq y$ implica $a^x = a^y$, allora f è un isomorfismo.
(6) 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.
(7) Mostrate che A ha un minimo m.
(8) 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 $m \leq n$.
   Questo m si dice *periodo* o *ordine* di a.
(9) Mostrate che si ha
$$\begin{cases} a^x = 1 & \text{se e solo se } m \mid x \\ a^x = a^y & \text{se e solo se } x \equiv y \pmod{m} \end{cases}$$
(10) 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.
(11) Mostrate che $\langle a \rangle$ è il più piccolo sottogruppo di G che contenga a.
(12) Mostrate che $\langle a \rangle$ ha m elementi, che sono
$$a^0 = 1, a^1 = a, a^2, \ldots, a^{m-1}.$$
(13) Trovate il periodo di
   (a) $[10]$ in $U(\mathbf{Z}/7\mathbf{Z})$,
   (b) $[10]$ in $U(\mathbf{Z}/13\mathbf{Z})$,
   (c) $[2]$ in $U(\mathbf{Z}/13\mathbf{Z})$.

Esercizio 9.2. Siano $(G, \cdot, 1)$ un gruppo, e $(M, \cdot, 1)$ un monoide.
Sia $f : G \to M$ un morfismo di monoidi, dunque

(1) $f(xy) = f(x)f(y)$ per $x, y \in G$, e
(2) $f(1) = 1$.

Si mostri che $f(G)$ è un sottogruppo del monoide M, cioè che ogni elemento $z \in f(G)$ ha un inverso $z^{-1} \in f(G)$. Più precisamente, si mostri che $f(x)^{-1} = f(x^{-1})$ per $x \in G$.

Esercizio 9.3. Sia G un gruppo, e si definiscano le traslazioni sinistre

$$\begin{aligned} \lambda(a) : G &\to G \\ x &\mapsto a \cdot x, \end{aligned}$$

per $a \in G$. Dunque λ definita da

$$\begin{aligned} \lambda : G &\to M(G) \\ a &\mapsto \lambda(a) \end{aligned}$$

è una funzione su G a valori nel monoide $M(G)$ delle funzioni su G.

(1) Si mostri che λ è un morfismo di monoidi, cioè
   (a) Si mostri che $\lambda(1) = \mathbf{1}_G$.
   (b) Si mostri che $\lambda(ab) = \lambda(a) \circ \lambda(b)$, per $a, b \in G$.
(2) Se ne deduca che ogni $\lambda(a)$ è una funzione invertibile, con $\lambda(a)^{-1} = \lambda(a^{-1})$.

Esercizio 9.4. Che succede nell'esercizio precedente se invece considero le traslazioni destre

$$\rho(a) : x \mapsto xa?$$

Esercizio 9.5. Mostrate che se G è un gruppo finito abeliano (cioè commutativo), allora per ogni $a \in G$ si ha

$$a^{|G|} = 1,$$

ovvero equivalentemente

$$|a| \text{ divide } |G|,$$

ove $|a|$ indica l'ordine/il periodo di a.

Esercizio 9.6. Enunciate e dimostrate il Teorema di Eulero-Fermat.

Esercizio 9.7. Enunciate e dimostrate il Piccolo Teorema di Fermat.

In particolare, a lezione vi ho dimostrato che se p è un numero primo, allora

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{per ogni } a \in \mathbf{Z} \text{ tale che } p \nmid a. \tag{1}$$

Ora mostrate che da questo segue che

$$a^p \equiv a \pmod{p} \quad \text{per ogni } a \in \mathbf{Z}. \tag{2}$$

Ora vi chiedo di vedere che da (2) segue (1), ma per la verità ve lo dico io. La ragione è che (2) afferma che

$$p \mid a(a^{p-1} - 1).$$

Dunque p, che è un numero primo, deve dividere uno dei fattori. Se $p \nmid a$, si ha dunque $p \mid a^{p-1} - 1$, cioè (1).

Esercizio 9.8. **Premessa.** Una frazione tipo $1/99$ si scrive come numero decimale periodico

$$0.01\,01\,01\,\ldots$$

Il numero decimale si ripete con lunghezza di periodo 2, ma naturalmente anche con lunghezza di periodo 4, 6, ecc. In generale si ripete ogni $2k$ cifre. Ma 2 è la *minima* lunghezza di periodo.

Sia ora n un numero intero positivo, con $\gcd(10, n) = 1$. Sia m il periodo di $[10]$ in $\mathbf{Z}/n\mathbf{Z}$.

Si mostri che la frazione $\dfrac{1}{n}$, scritta come numero decimale periodico, ha periodo lungo m.

Adesso vediamo che m è proprio la *minima* lunghezza di un periodo. Se infatti $1/n$ ha minima lunghezza del periodo k, e dunque

$$\frac{1}{n} = \frac{P}{10^k - 1},$$

ove P è il periodo, allora

$$10^k \equiv 1 \pmod{n},$$

e dunque $m \mid k$.

Esercizio 9.9.

(1) Si calcoli lo sviluppo decimale periodico di

$$\frac{1}{n},$$

per $n = 3, 7, 9, 11, 13, 17, 19$. Se ne discuta il legame con il periodo di $[10]$ in $U(\mathbf{Z}/n\mathbf{Z})$.

(2) Si calcoli lo sviluppo decimale periodico anche di

$$\frac{2}{7}, \frac{3}{7}, \frac{4}{7}, \frac{5}{7}, \frac{6}{7},$$

confrontandolo con quello di $\dfrac{1}{7}$.

(3) Facoltativamente, si calcoli anche lo sviluppo decimale periodico di $1/15$. (Per quest'ultimo, si possono vedere gli appunti.)