TRENTO, A.A. 2019/20
CORSO DI ALGEBRA A
FOGLIO DI ESERCIZI # 8

Esercizio 8.1. 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 $a \mapsto \lambda_a$ è una funzione $G \to G^G$.

(1) Si mostri che $\lambda_1 = \mathbf{1}_G$.
(2) Si mostri che $\lambda_{ab} = \lambda_a \circ \lambda_b$, per $a, b \in G$.
(3) Si mostri che ogni λ_a è una funzione invertibile, e $\lambda_a^{-1} = \lambda_{a^{-1}}$.
(4) Si mostri che

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

è un morfismo di gruppi, ove $S(G)$ è il gruppo delle funzioni invertibili (cioè biiettive) su G.

Esercizio 8.2 (Spoiler). Sia G un gruppo, e si definiscano le traslazioni destre

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

per $a \in G$. Dunque $a \mapsto \rho_a$ è una funzione $G \to G^G$.

(1) Si mostri che $\rho_1 = \mathbf{1}_G$.
(2) Si mostri che $\rho_{ab} = \rho_b \circ \rho_a$, per $a, b \in G$. (Avete notato l'ordine nella composizione?)
(3) Si mostri che ogni ρ_a è una funzione invertibile, e $\rho_a^{-1} = \rho_{a^{-1}}$.
(4) Si mostri che

$$\begin{aligned} \rho : G &\to S(G) \\ a &\mapsto \rho_a, \end{aligned}$$

è un *anti*morfismo di gruppi, nel senso anzidetto che $\rho_{ab} = \rho_b \circ \rho_a$.

Esercizio 8.3. 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 8.4. Enunciate e dimostrate il Teorema di Eulero-Fermat.

Esercizio 8.5. Enunciate e dimostrate il Piccolo Teorema di Fermat.

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

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

da cui ho fatto vedere che 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 8.6. **Premessa.** Una frazione tipo $1/99$ si scrive come numero decimale periodico

$$0.01\,01\,01\,\dots$$

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 8.7.

(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.)

Esercizio 8.8 (Serve per quello dopo).

(1) Siano G, H, K gruppi, $s : G \to H$ e $t : H \to K$ morfismi. Si mostri che $t \circ s : G \to K$ è un morfismo.
(2) Si formuli e si dimostri l'analogo risultato per gli anelli.
(3) Si mostri che la composizione di due isomorfismi (di gruppi, di anelli) è ancora un isomorfismo.

    (SUGGERIMENTO: Che la composizione sia un morfismo l'abbiamo visto nei due punti precedenti. Resta da vedere che la composizione di due funzioni biiettive sia ancora una funzione biiettiva, e questo si può fare ad esempio ricorrendo al fatto che una funzione è biiettiva se e solo se è invertibile (sia a destra che a sinistra).)
(4) Siano G, H gruppi, $s : G \to H$ un morfismo. Supponiamo che s sia un isomorfismo, cioè anche una funzione biiettiva; dunque esiste la funzione inversa $s^{-1} : H \to G$. Si mostri che s^{-1} è un morfismo, e quindi anche s^{-1} è un isomorfismo.

    (SUGGERIMENTO: Devo mostrare che per $x, y \in H$ si ha $s^{-1}(xy) = s^{-1}(x)s^{-1}(y)$. Dato che s è iniettiva, è sufficiente mostrare che $s(s^{-1}(xy)) = s(s^{-1}(x)s^{-1}(y))$. E in effetti $s(s^{-1}(xy)) = xy$ per definizione di funzione inversa, mentre dato che s è un morfismo, si ha $s(s^{-1}(x)s^{-1}(y)) = s(s^{-1}(x))s(s^{-1}(y)) = xy$.)
(5) Si formuli e si dimostri l'analogo risultato per gli anelli.

Esercizio 8.9. Questo esercizio vuole chiarire perché si usa (e ho usato anch'io) il termine *a ha periodo* 0 per un elemento a di un gruppo G tale che le potenze di a siano tutte distinte.

La ragione è che quando le potenze di a non sono tutte distinte, abbiamo visto che c'è un intero $m > 0$ che è il periodo/ordine di a, e che la funzione

$$\begin{aligned} \mathbf{Z}/m\mathbf{Z} &\to \langle\, a \,\rangle \\ [x] &\mapsto a^x \end{aligned} \tag{3}$$

è un isomorfismo.

Quando le potenze di a sono tutte distinte, abbiamo visto invece che la funzione

$$\begin{aligned} f : \mathbf{Z} &\to \langle\, a \,\rangle \\ x &\mapsto a^x \end{aligned}$$

è un isomorfismo.

Ora $\mathbf{Z}/m\mathbf{Z}$ è l'insieme delle classi di congruenza modulo $m > 0$. Ricordate che abbiamo visto che la congruenza modulo 0 non è altro che l'eguaglianza, cioè per $x, y \in \mathbf{Z}$

$$x \equiv y \pmod{0} \iff x = y.$$

Dunque le classi di congruenza modulo 0 non sono altro che, per $a \in \mathbf{Z}$,

$$[x] = \{\, y \in \mathbf{Z} : y = x \,\} = \{\, x \,\}$$

i sottoinsiemi di $\mathbf{Z}$ con un solo elemento. Dunque l'insieme delle classi di congruenza modulo 0 è, secondo la notazione che abbiamo usato

$$\mathbf{Z}/0\mathbf{Z} = \{ \{ x \} : x \in \mathbf{Z} \} .$$

Non ci vuole molto a capire che la funzione

$$\begin{aligned} q : \mathbf{Z} &\to \mathbf{Z}/0\mathbf{Z} \\ x &\mapsto [x] \end{aligned}$$

è un isomorfismo; l'unica differenza fra i due gruppi è che in quello di destra intero è circondato da parentesi quadre. A questo punto, usando l'Esercizio 8.8, otteniamo che la funzione

$$\begin{aligned} f \circ q^{-1} : \mathbf{Z}/0\mathbf{Z} &\to \langle a \rangle \\ [x] &\mapsto a^x \end{aligned}$$

è un isomorfismo.

Dunque l'isomorfismo (3) vale anche per $m = 0$, ed è per questo che se le potenze di a sono tutte distinte, si usa dire che a ha periodo zero.

Esercizio 8.10. Decifrate i testi seguenti, che sono stati cifrati col cifrario di Cesare C_t, per vari valori di t.

- `LCJKCXXMBCJAYKKGLBGLMQRPYTGRY`
- `UGFWVQKPSWGNECHHGKQPQPRGPUCXQ`
- `CGMZFUBUMFFUEBADOTUPMXMHMDQ`