Corso di Laurea in Informatica
Algebra. a.a. 2023-24. Proff. P. Piazza e G. Viaggi
Teorema di struttura per i gruppi ciclici

Abbiamo visto, e trovate tutti i dettagli in Schoof-Van Geemen, [S-VG], Teorema 3.6, pagina 24, che

- se $d \in \mathbb{Z}$, allora $d\mathbb{Z} \equiv \{dk, k \in \mathbb{Z}\} \subset (\mathbb{Z}, +)$ è un sottogruppo di $(\mathbb{Z}, +)$; viceversa, se $H \leq (\mathbb{Z}, +)$, allora esiste $d \in \mathbb{Z}$ tale che $H = d\mathbb{Z}$. Inoltre se $d \neq d'$ allora i due sottogruppi corrispondenti sono distinti.
- se $d \in \mathbb{Z}$ è un divisore di n e $n/d = k$ allora $H_d = \{[d], [2d], \ldots, [(k-1)d], [0]\}$ è un sottogruppo di $(\mathbb{Z}_n, +)$ di ordine k; viceversa se $H \leq (\mathbb{Z}_n, +)$, allora esiste un divisore di n, d, con $n = dk$, tale che $H = H_d$. Inoltre se d e d' sono due divisori distinti di n allora $H_d \neq H_{d'}$.

Osserviamo che sia $(\mathbb{Z}, +)$ che $(\mathbb{Z}_n, +)$ sono gruppi ciclici; il primo generato da $1 \in \mathbb{Z}$ ed il secondo generato da $[1] \in \mathbb{Z}_n$. Notiamo anche che i sottogruppi di $(\mathbb{Z}, +)$ sono tutti ciclici, perché $d\mathbb{Z}$ è generato da d; similmente i sottogruppi di $(\mathbb{Z}_n, +)$ sono tutti ciclici, perché H_d, con $n = kd$, è ciclico di ordine k ed è generato da $[d] = [n/k]$.
Abbiamo poi visto che se G è ciclico, $G = \langle g \rangle \equiv \{g^t, t \in \mathbb{Z}\}$, allora

- se g ha ordine ∞ allora esiste un isomorfismo di gruppi $\phi : (\mathbb{Z}, +) \to (G, \cdot)$ dato da $\phi(m) := g^m$;
- se g ha ordine n allora esiste un isomorfismo $\phi : (\mathbb{Z}_n, +) \to (G, \cdot)$ dato da $\phi([m]) = g^m$.

Si veda [S-VG], Teorema 5.7.

Un isomorfismo $\phi : G \to G'$ fra due gruppi è tale che il suo inverso insiemistico, $\phi^{-1} : G' \to G$, è anche un isomorfismo di gruppi [1]. Inoltre sappiamo che l'immagine tramite un omomorfismo di un sottogruppo è un sottogruppo. Tutto ciò vuol dire che un isomorfismo $\phi : G \to G'$ stabilisce un corrispondenza biunivoca fra i sottogruppi di G ed i sottogruppi di G': infatti, se $H \leq G$ allora $H = \phi^{-1}(\phi(H))$ e sappiamo che $\phi(H)$ è un sottogruppo.
Sappiamo anche, era un esercizio del compito a casa del 3/11/23, che un isomorfismo preserva l'ordine di un elemento e quindi trasforma un sottogruppo ciclico di ordine n di G in un sottogruppo ciclico di ordine n di G'; similmente, trasforma un sottogruppo ciclico di ordine infinito di G in un sottogruppo ciclico di ordine infinito di G'.

Alla luce di tutte queste informazioni abbiamo allora il seguente

Teorema di struttura per i gruppi ciclici.

(1) Se G è un gruppo ciclico e $H \leq G$ allora H è ciclico;
(2) se G è generato da un elemento di ordine n, $G = \langle g \rangle$ e $g^n = 1_G$, allora se $H \leq G$ l'ordine di H divide n [2];
(3) se G è generato da un elemento di ordine n, $G = \langle g \rangle$ e $g^n = 1_G$, allora esiste un corrispondenza biunivoca fra i divisori k di n, $n = kd$, ed i sottogruppi di ordine k di G; questa corrispondenza associa a k divisore di n il sottogruppo $\langle g^{\frac{n}{k}} \rangle$;

[1] Esercizio. Soluzione in [S-VG], Teorema 3.12, (ii)
[2] questo segue anche dal Teorema di Lagrange perché $|G| = n$, ma qui lo vediamo direttamente

(4) se k divide n e h divide k allora $\langle g^{\frac{n}{h}} \rangle$ è un sottogruppo ciclico di $\langle g^{\frac{n}{k}} \rangle$.

Dimostrazione.
(1) Abbiamo visto che esiste un isomorfismo $\phi : \mathbb{Z} \to G$ oppure $\phi : \mathbb{Z}_n \to G$ a seconda che G sia generato da un elemento di ordine infinito o di ordine n. Sia ψ l'inverso di ϕ, anche un isomorfismo di gruppi. Se $H \leq G$ allora $H = \phi(\psi(H))$; ma $\psi(H)$ è ciclico, perché è un sottogruppo di $\mathbb{Z}$ oppure di $\mathbb{Z}_n$ e sappiamo che tutti i sottogruppi di $\mathbb{Z}$ o $\mathbb{Z}_n$ sono ciclici; quindi H, come immagine tramite un isomorfismo ϕ di un sottogruppo ciclico, è necessariamente ciclico.
(2) se $H \leq G$ allora sappiamo che esiste d, con $n = dk$, tale che $H = \phi(H_d)$; ma H_d ha ordine k e H ha lo stesso ordine di H_d; quindi l'ordine di H divide n.
(3) sappiamo che esiste d, con $n = dk$, tale che $H = \phi(H_d)$; ma allora $H = \langle g^d \rangle \equiv \langle g^{\frac{n}{k}} \rangle$; quindi dato un sottogruppo H esiste un divisore di n, k, tale che $H = \langle g^{\frac{n}{k}} \rangle$; viceversa, se k è un divisore di n, $n = kd$, allora $H_{\frac{n}{k}} \equiv H_d$ è un sottogruppo di $\mathbb{Z}_n$ e quindi $\phi(H_{\frac{n}{k}}) = \langle g^{\frac{n}{k}} \rangle$ è un sottogruppo di G.
(4) sappiamo che $\langle g^{\frac{n}{k}} \rangle$ è un sottogruppo ciclico di ordine k di G; in particolare è esso stesso un gruppo ciclico di ordine k; quindi se h divide k allora per (3) esiste un sottogruppo ciclico di $\langle g^{\frac{n}{k}} \rangle$ di ordine h e questo sottogruppo è necessariamente $\langle g^{\frac{n}{h}} \rangle$; infatti, sempre per (3) sappiamo che tale sottogruppo è dato da $\langle (g^{\frac{n}{k}})^{\frac{k}{h}} \rangle$ ma questo sottogruppo è proprio $\langle g^{\frac{n}{h}} \rangle$.
La dimostrazione è completa.