Esercizi 7.7–7.10

Testo e soluzioni dettagliate

Dal capitolo 7 di A. Loi, *Appunti sulla teoria elementare dei gruppi*

Esercizio 7.7

Enunciato

Sia G un gruppo e siano $a, b \in G$ elementi di ordine finito che commutano. Supponendo che $(o(a), o(b)) = 1$, dimostrare che

$$o(ab) = o(a)o(b).$$

(Suggerimento: se $(ab)^t = 1$, dedurre da $a^t = b^{-t}$ che $o(a) \mid t$ e $o(b) \mid t$.)

Soluzione

Poniamo $m = o(a)$, $n = o(b)$ e $d = o(ab)$. Per ipotesi $(m, n) = 1$ e $ab = ba$. Si ha quindi

$$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = 1,$$

per cui $d \mid mn$.

D'altra parte, dall'uguaglianza $(ab)^d = 1$ e dalla commutatività tra a e b segue $a^d = b^{-d}$. Elevando i due membri alla potenza n otteniamo $a^{dn} = 1$, quindi $m \mid dn$. Poiché $(m, n) = 1$, ne deduciamo $m \mid d$. Analogamente, elevando alla potenza m otteniamo $b^{dm} = 1$ e dunque $n \mid dm$; ancora per $(m, n) = 1$ segue $n \mid d$. Essendo m e n coprimi, risulta $mn \mid d$. In conclusione $d \mid mn$ e $mn \mid d$, ossia

$$\boxed{o(ab) = d = mn = o(a)o(b).}$$

Esercizio 7.8

Enunciato

1. Sia G un gruppo e siano $a, b \in G$ elementi di ordine finito che commutano. Dimostrare che esiste $z \in \langle a, b \rangle$ tale che

   $$o(z) = \operatorname{mcm}\big(o(a), o(b)\big).$$

   (Suggerimento: scrivere $o(a) = m$ e $o(b) = n$; distribuire tra due divisori coprimi di m e n le massime potenze dei primi che compaiono in m oppure in n, e applicare l'Esercizio 7.7.)

2. Sia G un gruppo abeliano finito e sia $x \in G$ un elemento di ordine massimo k. Dedurre dal punto precedente che

   $$o(y) \mid k \qquad \text{per ogni } y \in G.$$

Soluzione

1. Poniamo $m = o(a)$, $n = o(b)$ e indichiamo con $\mathcal{P}$ l'insieme dei primi che dividono m oppure n. Scriviamo

   $$m = \prod_{p \in \mathcal{P}} p^{\alpha_p}, \qquad n = \prod_{p \in \mathcal{P}} p^{\beta_p},$$

   dove $\alpha_p, \beta_p \geq 0$. Consideriamo i divisori

   $$m' = \prod_{\substack{p \in \mathcal{P} \\ \alpha_p \geq \beta_p}} p^{\alpha_p}, \qquad n' = \prod_{\substack{p \in \mathcal{P} \\ \beta_p > \alpha_p}} p^{\beta_p}.$$

Per costruzione, $m' \mid m$ e $n' \mid n$. Inoltre, nessun primo divide entrambi m' e n', perciò $\gcd(m', n') = 1$. Per ogni $p \in \mathcal{P}$ compare in $m'n'$ esattamente la maggiore tra le potenze di p in m e in n; pertanto

$$m'n' = \prod_{p \in \mathcal{P}} p^{\max\{\alpha_p, \beta_p\}} = \operatorname{mcm}(m, n).$$

Poniamo

$$u = a^{m/m'}, \qquad v = b^{n/n'}.$$

Usando la formula per l'ordine di una potenza, otteniamo

$$o(u) = \frac{m}{\gcd(m, m/m')} = m', \qquad o(v) = \frac{n}{\gcd(n, n/n')} = n'.$$

Gli elementi u e v commutano perché sono potenze di a e b, e hanno ordini coprimi. Per l'esercizio 7.7, applicato a u e v, si ha

$$o(uv) = o(u)o(v) = m'n' = \operatorname{mcm}(m, n).$$

Dunque $z = uv \in \langle a, b \rangle$ è l'elemento cercato.

2. Sia $y \in G$. Poiché G è abeliano, x e y commutano; il punto precedente assicura che esiste $z \in \langle x, y \rangle \subseteq G$ con

$$o(z) = \operatorname{mcm}(o(x), o(y)) = \operatorname{mcm}(k, o(y)).$$

Per la scelta di k come ordine massimo, $o(z) \leq k$; d'altra parte, il minimo comune multiplo è un multiplo di k. Quindi

$$k \leq \operatorname{mcm}(k, o(y)) = o(z) \leq k,$$

da cui $\operatorname{mcm}(k, o(y)) = k$, ossia $o(y) \mid k$. Essendo y arbitrario, la tesi è dimostrata.

Esercizio 7.9

Enunciato

Sia $\mathbb{K}$ un campo e sia $G \leq \mathbb{K}^*$ un sottogruppo finito. Posto $k = \max\{o(a) \mid a \in G\}$, dimostrare che:

1. $a^k = 1$ per ogni $a \in G$;
2. $|G| \leq k$, considerando le radici in $\mathbb{K}$ del polinomio $T^k - 1$;
3. G è ciclico.

(Suggerimento: scegliere $x \in G$ con $o(x) = k$ e confrontare $|G|$ con $|\langle x \rangle|$.)

Soluzione

Il gruppo moltiplicativo $\mathbb{K}^*$ è abeliano, quindi anche G è abeliano. Essendo G finito, il massimo k degli ordini dei suoi elementi esiste.

1. Per il secondo punto dell'esercizio 7.8, applicabile a G in quanto gruppo abeliano finito, l'ordine di ogni $y \in G$ divide k. Di conseguenza $y^k = 1$ per ogni $y \in G$.

2. Tutti gli elementi di G sono allora radici del polinomio

$$f(T) = T^k - 1 \in \mathbb{K}[T].$$

Poiché $\mathbb{K}$ è un campo, un polinomio non nullo di grado k ha al più k radici distinte. Ne segue $|G| \leq k$.

3. L'elemento x scelto prima ha ordine k, quindi $|\langle x\rangle| = k$. Essendo $\langle x\rangle \leq G$,

$$k = |\langle x\rangle| \leq |G| \leq k.$$

Pertanto $G = \langle x\rangle$ ed è ciclico.

Esercizio 7.10

Enunciato

Sia p un numero primo dispari.

1. Applicando l'esercizio precedente al campo $\mathbb{Z}_p$, dimostrare che $\mathrm{Aut}(\mathbb{Z}_p)$ è ciclico e ha ordine $p-1$.
2. Trovare un generatore di $U(\mathbb{Z}_p, \cdot)$ per $p = 5$, $p = 7$ e $p = 11$, verificandone l'ordine.

Soluzione

1. Poiché p è primo, il gruppo delle unità di $\mathbb{Z}_p$ coincide con il gruppo moltiplicativo del campo $\mathbb{Z}_p$, cioè

$$U(\mathbb{Z}_p, \cdot) = \mathbb{Z}_p \setminus \{[0]_p\}, \qquad |U(\mathbb{Z}_p, \cdot)| = p - 1.$$

Per l'esercizio 7.9, questo gruppo è ciclico. L'isomorfismo $\mathrm{Aut}(\mathbb{Z}_p) \cong U(\mathbb{Z}_p, \cdot)$, già dimostrato negli appunti, implica pertanto che $\mathrm{Aut}(\mathbb{Z}_p)$ è ciclico, di ordine $p-1$.

2. Verifichiamo direttamente gli ordini dei seguenti elementi.

- $p = 5$**.** Per $[2]_5$ si ha

$$2^2 \equiv 4 \not\equiv 1 \pmod 5, \qquad 2^4 \equiv 1 \pmod 5.$$

Poiché l'ordine divide 4 e non è 1 né 2, si ha $o([2]_5) = 4 = p - 1$.

- $p = 7$**.** Per $[3]_7$ si ha

$$3^2 \equiv 2 \not\equiv 1 \pmod 7, \qquad 3^3 \equiv 6 \not\equiv 1 \pmod 7, \qquad 3^6 \equiv 1 \pmod 7.$$

L'ordine divide 6 ma non è 1, 2 né 3. Quindi $o([3]_7) = 6 = p - 1$.

- $p = 11$**.** Per $[2]_{11}$ si ha

$$2^2 \equiv 4 \not\equiv 1 \pmod{11}, \quad 2^5 \equiv 10 \not\equiv 1 \pmod{11}, \quad 2^{10} \equiv 1 \pmod{11}.$$

L'ordine divide 10 ma non è 1, 2 né 5. Perciò $o([2]_{11}) = 10 = p - 1$.

In ogni caso l'elemento individuato ha ordine uguale alla cardinalità del gruppo: si tratta quindi di un generatore.