آموزش ترجمه متون ریاضی (۱۰)

● حمید رضاامیری

Definition 2.31. Order of an element :
Let G be a group and let $a \in G$. Then a is said to be of *finite order* n, if n is the least positive integer such that $a^n = e$, the identity of G.

If for no positive integer k, $a^k = e$, then a is said to be of *infinite order*.

The symbol $o(a)$ shall denote the order of a.

تعریف ۲.۳۱. مرتبهٔ یک عضو

فرض کنیم G یک گروه و $a \in G$ باشد. دراین‌صورت a از مرتبهٔ متناهی n خوانده می‌شود، اگر n کوچکترین عدد صحیح و مثبتی باشد که $a^n = e$، و e عضو همانی G است.

اگر برای هیچ عدد صحیح و مثبت مانند k، $a^k = e$ برقرار نباشد، در این صورت a را از مرتبهٔ نامتناهی می‌گوییم.

نماد $o(a)$ برای نمایش مرتبهٔ a به کار می‌رود.

Definition 2.32. Cyclic Subgroup : A group G is said to be a cyclic group if there exists an element $b \in G$, such that every element of G is a power of b. Then b is called a *generator* of G and we denote G by $< b >$.

If the composition in G were denoted additively then we could say that G is a cyclic group if there exists an element a of G such that every element of G is of the form na where n is an integer.

تعریف ۲.۳۲. زیرگروه دوری

گروه G را یک گروه دوری می‌گوییم اگر عضوی چون $b \in G$ وجود داشته باشد، به قسمی که هر عضو G توانی از b باشد. دراین‌صورت b را مولد گروه G نامیده و G را به‌صورت $< b >$ نشان می‌دهیم.

هرگاه عمل تعریف شده در G یک عمل جمعی باشد، دراین‌صورت اگر عضوی از G مانند a وجود داشته‌باشد به قسمی که هر عضو G به شکل na که n یک عدد صحیح است، نوشته شود، می‌توانیم G را یک گروه دوری بنامیم.

EXAMPLE 22. Let $G_n = \left\{ e^{\frac{2\pi r i}{n}} \mid r = 0, 1, 2, \ldots, n-1 \right\}$ be the group of nth roots of unity. Let $a = e^{\frac{2\pi i}{n}}$, then $a \in G$. Since for any integer r, $e^{\frac{2\pi r i}{n}} = \left(e^{\frac{2\pi i}{n}} \right)^r = a^r$, every element of G is a power of a. Hence G_n is a cyclic group generated by a.

مثال ۲۲. فرض‌کنیم $G_n = \{ e^{\frac{2\pi r i}{n}} \mid r = 0, 1, 2, \ldots, n-1 \}$ گروهی حاصل از n امین ریشه‌های واحد باشد. فرض‌کنیم $a = e^{\frac{2\pi i}{n}}$، در این صورت $a \in G$. چون برای هر عدد صحیح r، $e^{\frac{2\pi r i}{n}} = (e^{\frac{2\pi i}{n}})^r = a^r$، هر عضو از G_n توانی از a است. بنابراین G_n یک گروه دوری تولید شده توسط a است.

EXAMPLE 23. The additive group $\mathbf{Z}$ is a cyclic group generated by 1, since $1 \in \mathbf{Z}$ and for every integer n, we have $n = n1$.

مثال ۲۳. گروه جمعی Z یک گروه دوری تولید شده توسط ۱ است، زیرا $1 \in Z$ و برای هر عدد صحیح مانند n، داریم: $n = n \times 1$.

Theorem 2.33. Order of a cyclic group is equal to the order of its generator.

(۱) قضیهٔ ۲.۳۳. *مرتبهٔ یک گروه دوری با مرتبهٔ مولّدش برابر است.*

---

(۱) به‌دلیل طولانی بودن اثبات و تاحدودی قابل استفاده نبودن آن برای دانش‌آموزان از آوردن اثبات خودداری شده‌است.

Now let G be any group and $a \in G$. Let $H=\{a^n \mid n \text{ is any positive integer}\}$. Consider any two elements $x=a^n$, $y=a^m$ in H. We find that $xy^{-1}=a^n a^{-m}=a^{n-m} \in H$. This implies that H is subgroup of G. Clearly H is a cyclic group generated by a. This subgroup is called a *cyclic subgroup* of G generated by a and we write $H=\langle a \rangle$.

حال فرض کنیم G گروهی دلخواه بوده و $a \in G$. فرض کنیم $H=\{a^n \mid n \in \mathbb{N}\}$ و $x=a^n$ دو عضو دلخواه مانند و $y=a^m$ در H در نظر می‌گیریم. در می‌یابیم که $xy^{-1}=a^n a^{-m}=a^{n-m} \in H$ این ثابت می‌کندکه H یک زیر گروه G است. واضح است که H یک گروه دوری تولید شده توسط a می‌باشد. این زیر گروه یک زیر گروه دوری از G نامیده می‌شود که توسط a تولید شده، می‌نویسیم $H=\langle a \rangle$.

Theorem 2.34. If G is a finite group then order of any element of G divides the order of G.

Proof: Let G be a finite group and $a \in G$. Let $H=\langle a \rangle$ be the cyclic subgroup of G generated by a

Then $o(H)=o(a)$ (Theorem 2.33).

By Lagrange's theorem $o(H) \mid o(G)$. Hence $o(a) \mid o(G)$. ■

قضیهٔ ۲.۳۴. اگر G یک گروهِ متناهی باشد در این صورت مرتبهٔ هر عضو از G مرتبهٔ G را عاد می‌کند (می‌شمارد).

اثبات: فرض کنیم G یک گروه متناهی و $a \in G$. فرض کنیم $H=\langle a \rangle$ یک زیر گروه دوریِ G و تولید شده توسط a باشد.

در این صورت $o(H)=o(a)$ (قضیهٔ ۲.۳۳).

از طرفی طبق قضیهٔ لاگرانژ[۲] $o(H) \mid o(G)$. بنابراین $o(a) \mid o(G)$. ■

Corollary 2.35. If G is a finite group then for any $a \in G$

$$a^{o(G)}=e.$$

Proof: Let $o(a)=n$ and $o(G)=N$.

Because of Theorem 2.3, $N=nm$ for some positive integer m. Then $a^N=(a^n)^m=e^m=e$.

Hence the corollary. ■

نتیجهٔ ۲.۳۵. اگر G یک گروه متناهی باشد در این صورت برای هر $a \in G$، $a^{o(G)}=e$.

(۲) طبق قضیهٔ لاگرانژ مرتبهٔ زیر گروه هر گروه، مرتبهٔ آن گروه راعاد می‌کند.

اثبات: فرض کنیم $o(G)=N$ ، $o(a)=n$.

طبق قضیهٔ ۲.۳۴، $(o(a) \mid o(G) \Rightarrow n \mid N \Rightarrow N=nm)N=nm$

به‌ازای عددی صحیح ومثبت مانند m. پس $a^N=(a^n)^m=e^m=e$

بنابراین نتیجه حاصل شد. ■

Theorem 2.36. In a group G, following hold:

(1) For any two elements $a, x \in G$, $o(a)=o(x^{-1}ax)$.

(2) If for any $a \in G$, $o(a)$ is finite; then for any integer m, $a^m=e$ implies $o(a) \mid m$.

(3) For any two elements $a, b \in G$, $o(ab)=o(ba)$.

(4) If $o(a)=n$ and a positive integer $k \mid n$, then

$$o(a^k)=\frac{n}{k}.$$

قضیهٔ ۲.۳۶. در یک گروه مانند G گزاره‌های زیر صدق می‌کنند.

(۱) برای هر دو عضو از G مانند a و x، $o(a)=o(x^{-1}ax)$

(۲) اگر برای هر $a \in G$ ، $o(a)$ متناهی باشد، در این صورت برای هر عدد صحیح m ، که $a^m=e$ ، ایجاب می‌کند اینکه $o(a) \mid m$.

(۳) برای هر دو عضو از G مانند a و b ، $o(ab)=o(ba)$.

(۴) اگر $o(a)=n$ و عددی صحیح و مثبت مانند k ، n را عاد کند $(k \mid n)$ ، در این صورت $o(a^k)=\frac{n}{k}$.

Proof: (1) Let n be any positive integer

$$a^n=e \Leftrightarrow x^{-1}a^n x=x^{-1}ex=e \Leftrightarrow (x^{-1}ax)^n=e,$$

since $(x^{-1}ax)^n=x^{-1}a^n x$.

Consequently $o(a)=o(x^{-1}ax)$.

(2) Let $o(a)=n$ and let m be any integer such that $a^m=e$.

اثبات: (۱) فرض کنیم n عددِ صحیحِ مثبت و دلخواهی باشد و $(a^n=e)$.

$$a^n=e \Leftrightarrow x^{-1}a^n x=x^{-1}ex=e \Leftrightarrow (x^{-1}ax)^n=e$$

زیرا $(x^{-1}ax)^n=x^{-1}a^n x$ (به‌استقراء می‌توان ثابت کرد).

بدین ترتیب (ثابت شد) $o(a)=o(x^{-1}ax)$.

(۲) فرض کنیم؛ $o(a)=n$ و فرض کنیم m عددی صحیح و دلخواه باشد به قسمی که $a^m=e$.

Now by Euclid's algorithm $m=nq+r$ for some integers q and r with $0 \leqslant r < n$.
Then $e=a^m=(a^n)^q a^r=e^q a^r=ea^r=a^r$.
But n is the least positive integer such that $a^n=e$ and $r < n$.
Hence $r=0$ and so $m=nq$ i.e., $o(a)=n \mid m$. This proves (2).
(3) Since $ab=b^{-1}(ba)b$, $o(ab)=o(ba)$ by part (1).
(4) follows from (2).■

حال باتوجه به الگوریتم اقلیدسی داریم، $m = nq + r$ که r و q اعدادی صحیح و $0 \leq r < n$.

بنابراین: $e = a^m = (a^n)^q \cdot a^r = e^q a^r = ea^r = a^r$. (ثابت شد $a^r = e$) اما از طرفی n کوچکترین عدد صحیح و مثبتی است (طبق تعریف مرتبه برای a) که $a^n = e$ و $r < n$.

بنابراین باید $r = 0$ پس $m = nq$ یعنی؛ $o(a) = n \mid m$. این مطلب (۲) را اثبات می‌کند.

(۳) چون $ab = b^{-1}(ba)b$، باتوجه به (۱) $o(ab) = o(ba)$.

(۴) از (۲) نتیجه می‌شود. ■

(*i*) $i^4=1$ but for no positive integer $m < 4$
$i^m=1$. This means $o(i)=4$. Trivially $4 \mid o(G)$.
(*ii*) Now $(-1)^2=1$ and $(-1)^1 \neq 1$. This implies $o(-1)=2$. Clearly $o(-1) \mid o(G)$.
(*iii*) Since $1=i^4$, $-1=i^2$, $-i=i^3$, $i=i$ we see that G is a cyclic group generated by i. Notice that G is also generated by $-i$ But -1 or 1 do not generate G.

I) $i^4 = 1$، اما برای اعدادی مثبت چون $m < 4$، $i^m = 1$ برقرار نیست. این به معنی آن است که $o(i) = 4$. بدیهی است که $4 \mid o(G)$.

II) حال داریم، $(-1)^2 = 1$ و $(-1)^1 \neq 1$. این ایجاب می‌کند که $o(-1) = 2$. واضح است که $o(-1) \mid o(G)$.

III) از آن‌جایی که $i^4 = 1$ و $i^2 = -1$ و $i^3 = -i$ و $i = i$، مشاهده می‌کنیم که G گروهی است دوری، تولید شده توسط i. توجه داریم که همچنین G توسط $-i$ می‌تواند تولید شود امّا -1 یا 1 نمی‌توانند G را تولید کنند.

EXAMPEE 24. Consider the group $G=\{1, -1, i, -i\}$ where $i=\sqrt{-1}$. Now $o(G)=4$.

مثال ۲۴. گروه $G = \{1, -1, i, -i\}$ را که در آن $i = \sqrt{-1}$، درنظر می‌گیریم. حال می‌دانیم $o(G) = 4$.

مسائل مسابقه‌ای

با استفاده از استقرای ریاضی ثابت کنید:

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^{n-r} b^r$$

(می‌دانیم: $\binom{n}{r} = \frac{n!}{r!(n-r)!}$)

تفریح اندیشه ۲

عدد 606 را بر تکه کاغذی نوشته‌ایم. برای این که عدد مزبور $\frac{۳}{۲}$ مرتبه بزرگتر شود چه عملی باید انجام گیرد؟

606

جواب در صفحهٔ ۸۸