Ред на елемент. Циклични групи.

Определение 1. *Нека G е група с неутрален елемент e, $g \in G$, $n \in \mathbb{Z} \setminus \{0\}$ е ненулево цяло число,а*

$$\operatorname{sign}(n) := \begin{cases} 1 & \text{за } n > 0, \\ -1 & \text{за } n < 0 \end{cases}$$

е знакът на n. Определяме

$$g^n := \begin{cases} e & \text{за } n = 0, \\ \underbrace{g^{\operatorname{sign}(n)} \dots g^{\operatorname{sign}(n)}}_{|n|} & \text{за } n \in \mathbb{Z} \setminus \{0\}. \end{cases}$$

Тук $g^1 := g$, а g^{-1} е обратният елемент на g.

Лема 2. (Правило за умножение на степени с равни основи:) *Ако G е група, $g \in G$ и $m, n \in \mathbb{N}$ са цели числа, то $g^m g^n = g^{m+n}$.*

Доказателство. Ако $m = 0$, то $g^{0+n} = g^n = e_G g^n = g^0 g^n$. Аналогично, $g^{m+0} = g^m = g^m e_G = g^m g^0$ за $n = 0$. Отсега нататък ще считаме, че $m, n \in \mathbb{Z} \setminus \{0\}$.

Ако $m, n \in \mathbb{Z} \setminus \{0\}$ имат един и същи знак $\operatorname{sign}(m) = \operatorname{sign}(n) = \varepsilon = \pm 1$, то

$$g^m g^n = \underbrace{g^\varepsilon \dots g^\varepsilon}_{|m|} \underbrace{g^\varepsilon \dots g^\varepsilon}_{|n|} = \underbrace{g^\varepsilon \dots g^\varepsilon}_{|m|+|n|} = g^{m+n},$$

защото $m + n = \varepsilon(|m| + |n|)$ за ненулеви цели числа m и n с един и същи знак ε.

Нека $m \in \mathbb{Z} \setminus \{0\}$ и $n \in \mathbb{Z} \setminus \{0\}$ имат различни знаци и $|m| \geq |n|$. Ако означим $\varepsilon = \operatorname{sign}(m)$, то $\operatorname{sign}(n) = -\varepsilon$ и

$$g^m g^n = \underbrace{g^\varepsilon \dots g^\varepsilon}_{|m|} \underbrace{g^{-\varepsilon} \dots g^{-\varepsilon}}_{|n|} = \underbrace{g^\varepsilon \dots g^\varepsilon}_{|m|-|n|} = g^{m+n},$$

вземайки предвид $m + n = \varepsilon(|m| - |n|)$ за ненулеви цели числа m, n с различни знаци, $|m| \geq |n|$ и $\operatorname{sign}(m) = \varepsilon$.

□

Лема 3. (Правило за степенуване на степен:) *Ако G е група, $g \in G$ и $m, n \in \mathbb{Z}$ са цели числа, то $(g^m)^n = g^{mn}$.*

Доказателство. Ако $n = 0$, то $g^{m.0} = g^0 = e_G = (g^m)^0$.

Ако $n \in \mathbb{N}$, то

$$(g^m)^n = \underbrace{g^m \dots g^m}_{n} = g^{\underbrace{m+\dots+m}_{n}} = g^{mn}.$$

За отрицателно цяло n пресмятаме, че

$$(g^m)^n = \underbrace{(g^m)^{-1} \dots (g^m)^{-1}}_{|n|} = \underbrace{g^{-m} \dots g^{-m}}_{|n|} = g^{\underbrace{(-m)+\dots+(-m)}_{|n|}} = g^{(-m)|n|} = g^{mn},$$

вземайки предвид $(g^m)^{-1} = g^{-m}$. Последното равенство следва от това, че $(g^m)^{-1} \in G$ е единственото решение на уравнението $g^m x = e_G$ от G и $g^m g^{-m} = g^{m+(-m)} = g^0 = e_G$, съгласно Лема 2 за умножение на степени с равни основи.

□

Нека G е група, $g \in G$. Ако съществува ненулево цяло число $m \in \mathbb{Z} \setminus \{0\}$ с $g^m = e_G$, то $g^{-m} = (g^m)^{-1} = e_G$ и съществува естествено число $n \in \mathbb{N}$ с $g^n = e_G$. Всяко множество от естествени числа е ограничено отдолу.

Определение 4. *Ако G е група, $g \in G$ и съществува ненулево цяло число $m \in \mathbb{Z} \setminus \{0\}$ с $g^m = e_G$ за неутралния елемент e_G на G, то минималното естествено $s \in \mathbb{N}$ с $g^s = e_G$ се нарича ред на g и се бележи с* $\operatorname{ord}(g) = s$.

Ако $g^m \neq e_G$ за всички $m \in \mathbb{Z} \setminus \{0\}$, то казваме че g е от безкраен ред и записваме $\operatorname{ord}(g) = \infty$.

Твърдим, че $\operatorname{ord}(g) = \infty$ тогава и само тогава, когато $g^m \neq g^n$ за всички различни цели числа $m, n \in \mathbb{Z}$. По-точно, ако $\operatorname{ord}(g) = \infty$ и допуснем, че $g^m = g^n$ за някои различни $m, n \in \mathbb{N}$, $m \neq n$, то $g^{m-n} = g^m g^{-n} = g^n g^{-n} = g^0 = e_G$ за $m - n \neq 0$ противоречи на определението за безкраен ред на елемента $g \in G$. Обратно, ако $g^m \neq g^n$ за всички различни цели числа $m, n \in \mathbb{Z}$, $m \neq n$, то за $n = 0$ и произволно $m \in \mathbb{Z} \setminus \{0\}$ получаваме $g^m \neq g^0 = e_G$ и стигаме до извода, че $\operatorname{ord}(g) = \infty$.

От гореспоменатия факт следва, че ако $g \in G$ е елемент от безкраен ред, то $\{g^m \mid m \in \mathbb{Z}\}$ е изоморфно като множество с $\mathbb{Z}$. В частност, ако $\operatorname{ord}(g) = \infty$, то $\{g^m \mid m \in \mathbb{Z}\}$ е безкрайно множество на G. Затова всеки елемент g на крайна група G е от краен ред $\operatorname{ord}(g) < \infty$. Безкрайна група може да има елементи както от краен, така и от безкраен ред. Например, безкрайната мултипликативна група $(\mathbb{C}^*, .)$ на полето $\mathbb{C}$ на комплексните числа има елемент $i = \sqrt{-1} \in \mathbb{C}$ от ред 4 и елемент $2 \in \mathbb{C}^*$ от безкраен ред. Тук използваме, че минималната степен на имагинерната единица $i = \sqrt{-1}$, равна на 1 е 4 и $2^m \neq 1 = 2^0$ за всички $m \in \mathbb{Z} \setminus \{0\}$.

Твърдение 5. *Нека G е група, $g \in G$ и $m \in \mathbb{Z} \setminus \{0\}$. В такъв случай, $g^m = e_G$ за неутралния елемент e_G на G тогава и само тагава, когато елементът g е от краен ред* $\operatorname{ord}(g) = s \in \mathbb{N}$, *делящ m.*

Доказателство. Ако $g^m = e$ за някое $m \in \mathbb{Z} \setminus \{0\}$, то $g \in G$ е елемент от краен ред $\mathrm{ord}(g) = s$. Делим $m = sq + r$ на s с частно $q \in \mathbb{Z}$ и остатък $r \in \mathbb{Z}$, $0 \leq r \leq s-1$ и получаваме, че

$$g^r = g^{m+s(-q)} = g^m (g^s)^{-q} = e.e^{-q} = e.$$

Съгласно избора на $\mathrm{ord}(g) = s$ като минималното естествено число с $g^s = e$, цялото число r не е естествено, т.е. $r = 0$ и s дели $m = sq$.

Ако $g \in G$ е от краен ред $\mathrm{ord}(g) = s$, делящ m, то $m = sq$ за някое $q \in \mathbb{Z}$ и

$$g^m = g^{sq} = (g^s)^q = e^q = e.$$

□

Твърдение 6. *Нека G е група, $g \in G$ е елемент от ред $\mathrm{ord}(g) = s \in \mathbb{N}$ и $k \in \mathbb{Z}$. Тогава елементът $g^k \in G$ е от ред*

$$\mathrm{ord}(g^k) = \frac{\mathrm{ord}(g)}{\mathrm{GCD}(\mathrm{ord}(g), k)} = \frac{s}{\mathrm{GCD}(s,k)}$$

за естествения най-голям общ делител $\mathrm{GCD}(s,k) \in \mathbb{N}$.

Доказателство. Означаваме

$$d := \mathrm{GCD}(s,k) \in \mathbb{N}, \quad s_1 := \frac{s}{d} \in \mathbb{N}, \quad k_1 := \frac{k}{d} \in \mathbb{Z}$$

и доказваме, че $\mathrm{ord}(g^k) = s_1$. От

$$(g^k)^{s_1} = g^{ks_1} = g^{k_1 d s_1} = g^{k_1 s} = (g^s)^{k_1} = e^{k_1} = e$$

следва, че $g^k \in G$ е от краен ред $t \in \mathbb{N}$, делящ s_1. Сега от

$$e = (g^k)^t = g^{kt} = g^{dk_1 t}$$

получаваме, че редът $s = ds_1$ на g дели $dk_1 t$. Следователно s_1 дели $k_1 t$ и поради взаимната простота на s_1 и k_1 стигаме до извода, че s_1 дели t. От t дели s_1 и s_1 дели t за естествените числа s_1 и t следва, че $\mathrm{ord}(g) = t = s_1$.

□

Лема-Определение 7. *Ако G е група и $g \in G$ е елемент на G, то подмножеството*

$$\langle g \rangle = \{g^m \mid m \in \mathbb{Z}\}$$

на G е абелева подгрупа, която се нарича циклична група, породена от g.

Доказателство. Наистина, за произволни $m, n \in \mathbb{Z}$ е в сила $g^m (g^n)^{-1} = g^m g^{-n} = g^{m-n} \in \langle g \rangle$, така че $\langle g \rangle$ е подгрупа на G. Съгласно $g^m g^n = g^{m+n} = g^{n+m} = g^n g^m$ за всички $m, n \in \mathbb{Z}$, подгрупата $\langle g \rangle$ на G е абелева.

□

Твърдение 8. *Нека G група и $g \in G$ е елемент на G. В такъв случай, g е от краен ред* $\mathrm{ord}(g) = s \in \mathbb{N}$ *тогава и само тогава, когато цикличната група $\langle g \rangle$, породена от g е от ред s и съвпада с множеството $\langle g \rangle = \{e, g, \ldots, g^{s-1}\}$. Ако това е изпълнено, то елемент $g^k \in \langle g \rangle$ поражда $\langle g \rangle$ тогава и само тогава, когато естественият най-голям общ делител на s и k е* $\mathrm{GCD}(s,k) = 1$.

Доказателство. Нека $g \in G$ е елемент от ред $\mathrm{ord}(g) = s \in \mathbb{N}$. Тогава за всяко цяло число $m \in \mathbb{Z}$, делението $m = sq + r$ на s с частно $q \in \mathbb{Z}$ и остатък $r \in \mathbb{Z}$, $0 \leq r \leq s-1$ дава

$$g^m = g^{sq+r} = g^{sq} g^r = (g^s)^q g^r = e^q g^r = g^r \in \{e, g, \ldots, g^{s-1}\},$$

така че

$$\langle g \rangle \subseteq \{e, g, \ldots, g^{s-1}\} \subseteq \{g^m \,|\, m \in \mathbb{Z}\} = \langle g \rangle$$

и $\langle g \rangle = \{e, g, \ldots, g^{s-1}\}$. Ако допуснем, че $g^i = g^j$ за $0 \leq i < j \leq s-1$, то $g^{j-i} = g^0 = e$, откъдето $s = \mathrm{ord}(g)$ дели $j - i$. Но единственото цяло число $-(s-1) \leq j - i \leq s-1$, кратно на s е $j - i = 0$. Противоречието доказва, че $g^i \neq g^j$ за всички $0 \leq i < j \leq s-1$ с цикличната група $\langle g \rangle = \{e, g, \ldots, g^{s-1}\}$, породена от g е от ред $s = \mathrm{ord}(g)$.

Ако цикличната група $\langle g \rangle$, породена от g е от ред $|\langle g \rangle| = s$, то $g \in G$ е от краен ред $t \in \mathbb{N}$, защото в противен случай от $\mathrm{ord}(g) = \infty$ следва $|\langle g \rangle| = \infty$. Съгласно доказаната посока, ако $\mathrm{ord}(g) = t$, то $\langle g \rangle$ е от ред $t = |\langle g \rangle| = s$.

В частност, ако $\mathrm{ord}(g) = |\langle g \rangle| = s$, то g^k поражда $\langle g \rangle = \langle g^k \rangle$ точно когато

$$s = \langle g^k \rangle = \mathrm{ord}(g^k) = \frac{s}{\mathrm{GCD}(s,k)}.$$

Последното е в сила точно когато естественият най-голям общ делител на s и k е $\mathrm{GCD}(s,k) = 1$.

□

Адитивната група $(\mathbb{Z}, +)$ на целите числа е циклична и се поражда от ± 1. Да отбележим, че в адитивен запис, цикличната подгрупа на $(\mathbb{Z}, +)$, породена от $m \in \mathbb{Z}$ е $m\mathbb{Z} = \{mz \,|\, z \in \mathbb{Z}\}$. При това, $m\mathbb{Z} = \mathbb{Z}$ тогава и само тогава, когато $m = \pm 1$, защото $1 \notin m\mathbb{Z}$ за $m \in \mathbb{Z}$ и $|m| \geq 2$ или $m = 0$.

За произволно естествено число n нека $\omega_n = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n} \in \mathbb{C}$. Множеството $\mathbb{C}_n = \{\omega_n^k \,|\, 0 \leq k \leq n-1\}$ на n-тите корени на единицата е циклична група, породена от ω_n. Съгласно Твърдение 8, елемент $\omega_n^k \in \mathbb{C}_n$ поражда $\mathbb{C}_n$ тогава и само тогава, когато естественият най-голям общ делител на k и n е $\mathrm{GCD}(k,n) = 1$.

Твърдение 9. *(i) Всяка безкрайна циклична група $\langle g \rangle = \{g^m \,|\, m \in \mathbb{Z}\}$ е изоморфна на адитивната група $(\mathbb{Z}, +)$ на целите числа.*

(ii) Нека $\omega_n = \cos\left(\frac{2\pi}{n}\right) + \sin\left(\frac{2\pi}{n}\right)$. Всяка циклична група $\langle g \rangle = \{e, g, \ldots, g^{n-1}\}$ от ред n е изоморфна на групата $\mathbb{C}_n = \{\omega_n^k \,|\, 0 \leq k \leq n-1\}$ на n-тите корени на единицата.

Доказателство. (i) Изображението

$$\varphi : \mathbb{Z} \longrightarrow \langle g \rangle = \{g^m \,|\, m \in \mathbb{Z}\},$$

$$\varphi(m) = g^m \quad \text{за всяко} \quad m \in \mathbb{Z}$$

е взаимно еднозначно, защото ако $\mathrm{ord}(g) = |\langle g\rangle| = \infty$, то $g^m \neq g^n$ за всички $m \neq n$, $m, n \in \mathbb{Z}$. Съгласно $\varphi(m+n) = g^{m+n} = g^m g^n = \varphi(m)\varphi(n)$ за произволни $m, n \in \mathbb{Z}$, изображението φ е хомоморфизъм, а оттам и изоморфизъм на групи.

(ii) Изображението

$$\psi : \mathbb{C}_n = \{\omega_n^r \,|\, 0 \leq r \leq n-1\} \longrightarrow \langle g\rangle = \{g^r \,|\, 0 \leq r \leq n-1\},$$

$$\psi(\omega_n^r) = g^r \quad \text{за всяко} \quad 0 \leq r \leq n-1$$

е взаимно еднозначно. За произволно $m \in \mathbb{Z}$, делението $m = nq + r$ на n с частно $q \in \mathbb{Z}$ и остатък $r \in \mathbb{Z}$, $0 \leq r \leq n-1$ дава

$$\omega_n^m = \omega_n^{nq+r} = \omega_n^{nq}\omega_n^r = (\omega_n^n)^q\omega_n^r = 1^q.\omega_n^r = 1.\omega_n^r = \omega_n^r$$

и

$$g^m = g^{nq+r} = g^{nq}g^r = (g^n)^q g^r = e^q g^r = e.g^r = g^r.$$

Следователно

$$\psi(\omega_n^m) = \psi(\omega_n^r) = g^r = g^m \quad \text{за произволно} \quad m \in \mathbb{Z}.$$

Оттук,

$$\psi(\omega_n^r\omega_n^s) = \psi(\omega_n^{r+s}) = g^{r+s} = g^r g^s = \psi(\omega_n^r)\psi(\omega_n^s)$$

за произволни $0 \leq r, s \leq n-1$ и ψ е биективен хомоморфизъм на групи, т.е. изоморфизъм на групи.

□

Лема 10. *Всяка подгрупа H на циклична група $G = \langle g\rangle$ е циклична. По-точно, $H = \{e_G\} = \langle e_G\rangle$ е тривиалната подгрупа или $H = \langle g^s\rangle$ се поражда от g^s за минималното естествено число $s \in \mathbb{N}$ с $g^s \in H$.*

Доказателство. Ако $H \neq \{e_G\}$ и $s \in \mathbb{N}$ е минималното естествено число, за което $g^s \in H$, то $\langle g^s\rangle \subseteq H$. По-точно, за всяко естестсвено $n \in \mathbb{N}$ имаме

$$(g^s)^n = \underbrace{g^s \ldots g^s}_{n} \in H \quad \text{и} \quad (g^s)^{-n} = \underbrace{(g^s)^{-1} \ldots (g^s)^{-1}}_{n} \in H,$$

защото $(g^s)^{-1} \in H$. За обратното включване $H \subseteq \langle g^s\rangle$ да вземем $g^m \in H$ с $m \in \mathbb{Z}$. Делението $m = sq + r$ на s с частно $q \in \mathbb{Z}$ и остатък $r \in \mathbb{Z}$, $0 \leq r \leq s-1$ дава

$$g^r = g^{m+s(-q)} = g^m g^{s(-q)} = g^m (g^s)^{-q} \in H.$$

Понеже $s \in \mathbb{N}$ е минималното естествено число с $g^s \in H$, цялото число r не е естествено, т.е. $r = 0$ и s дели $m = sq$. В резултат, $g^m = g^{sq} = (g^s)^q \in \langle g^s\rangle$. Това доказва $H \subseteq \langle g^s\rangle$ и $H = \langle g^s\rangle$.

□

Следствие 11. *Нека $G = \langle g\rangle = \{e, g, \ldots, g^{n-1}\}$ е циклична група от ред n и $H = \langle g^s\rangle \neq \{e_G\}$ е нетривиална подгрупа на G, породена от g^s за минималното естествено $s \in \mathbb{N}$ с $g^s \in H$. Тогава s дели n и $H = \langle g^s\rangle$ е подгрупа на G от ред $\frac{n}{s}$.*

Доказателство. Делим $n = sq + r$ на s с частно $q \in \mathbb{Z}$ и остатък $r \in \mathbb{Z}$, $0 \leq r \leq s-1$, за да забележим, че

$$g^r = g^{n+s(-q)} = g^n g^{s(-q)} = e_G (g^s)^{-q} = (g^s)^{-q} \in H,$$

вземайки предвид $g^n = e_G$. По предположение, $s \in \mathbb{N}$ е минималното естествено с $g^s \in H$, така че цялото число r не е естествено. Следователно $r = 0$ и s дели $n = sq$. В резултат, цикличната подгрупа $H = \langle g^s \rangle$ на $\langle g \rangle$ е от ред

$$|H| = \operatorname{ord}(g^s) = \frac{\operatorname{ord}(g)}{\operatorname{GCD}(\operatorname{ord}(g), s)} = \frac{n}{\operatorname{GCD}(n, s)} = \frac{n}{s}.$$

□

В означенията от Следствие 11, за произволно цяло $k \in \mathbb{Z}$, $\operatorname{GCD}\left(k, \frac{n}{s}\right) = \pm 1$ елементът g^{sk} поражда същата подгрупа $H = \langle g^s \rangle = \langle g^{sk} \rangle$. За степенния показател sk на пораждащия g^{sk} на H не можем да твърдим, че дели реда n на G.

Следствие 12. *Ако $G = \langle g \rangle = \{e_G, g, \ldots, g^{n-1}\}$ е циклична група от ред n, то за всеки естествен делител t на n съществува единствена подгрупа $H = \langle g^{\frac{n}{t}} \rangle$ на G от ред t.*

Доказателство. Подгрупата $H = \langle g^{\frac{n}{t}} \rangle$ на $G = \langle g \rangle$ е от ред

$$|H| = \operatorname{ord}(g^{\frac{n}{t}}) = \frac{\operatorname{ord}(g)}{\operatorname{GCD}(\operatorname{ord}(g), \frac{n}{t})} = \frac{n}{\operatorname{GCD}(n, \frac{n}{t})} = n : \left(\frac{n}{t}\right) = t.$$

Ако H_o е подгрупа от ред $|H_o| = t$ и $s \in \mathbb{N}$ е минималното естествено число с $g^s \in H_o$, то s дели n и $H_o = \langle g^s \rangle$ е от ред $t = |H_o| = \frac{n}{s}$, съгласно Следствие 11. Следователно $s = \frac{n}{t}$ и $H_o = \langle g^{\frac{n}{t}} \rangle = H$ е единствената подгрупа на G от ред t.

□

В означенията от Следствие 12 да забележим, че цикличната подгрупа $H = \langle g^{\frac{n}{t}} \rangle$ на $G = \langle g \rangle$ от ред t има най-различни пораждащи. За произволно цяло k, взаимно просто с t, елементът $g^{\frac{n}{t}k} \in H$ поражда $H = \langle g^{\frac{n}{t}k} \rangle$. Една и съща подгрупа H на G има различни пораждащи.