Циклични групи.

Нека G е група, $a \in G$. Разглеждам множеството

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}.$$

(Ако операцията в G е $+$, то разлгеждаме $\langle a \rangle = \{na \mid n \in \mathbb{Z}\}$.) От начина, по-който въведеохме груповите операции знаем, че $(a^n)^{-1} = a^{-n}$, $-n \in \mathbb{Z}$ и следователно $(a^n)^{-1} \in \langle a \rangle$; за $a^n, a^m \in \langle a \rangle$ имаме $a^n a^m = a^{n+m} = a^{m+n} = a^m a^n \in \langle a \rangle$. По този начин $\langle a \rangle$ е абелева подгрупа на G. Подгрупата $\langle a \rangle \leq G$ се нарича *циклична подгрупа на G, породена от a*. Ако за някой елемент $a \in G$ е изпълнено $\langle a \rangle = G$, то казваме, че групата G е *циклична*.

Примери:

1. Целите числа $\mathbb{Z}$ образуват група относно операцията събиране. Оказва се, че $\mathbb{Z}$ е циклична група. Наистина, за $\forall m \in \mathbb{Z}$ е изпълнено, че $m = m.1$ и следователно имаме $\mathbb{Z} = \langle 1 \rangle$[1].

2. Нека $n \in \mathbb{N}$ и $\mathbb{C}_n = \{z \in \mathbb{C} \mid z^n = 1\}$. Знаем, че $\mathbb{C}_n$ е група относно умножението от ред $|\mathbb{C}_n| = n$. Нека $\omega = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n} \in \mathbb{C}$. Тогава по формулата на Моавър намираме, че $\omega^n = \cos 2\pi + i \sin 2\pi = 1$ и следователно $\omega \in \mathbb{C}_n$. Но n-тите комплексни корени на единицата са $\cos 2k\pi n + i \sin 2k\pi n = \omega^k$ за $k = 0, 1, \ldots, n-1$ и следователно всички елементи на $\mathbb{C}_n$ са точно ω^k за $k = 0, 1, \ldots, n-1$, т.е. имаме че

$$\mathbb{C}_n = \left\{\omega^0 = 1, \omega, \omega^2, \ldots, \omega^{n-1}\right\}.$$

Така видяхме, че е изпълнено $\mathbb{C}_n = \langle \omega \rangle$ за $\omega \in \mathbb{C}_n$ и следователно $\mathbb{C}_n$ е циклична група (която също е абелева).

[1] Също така лесно се вижда и, че $\mathbb{Z} = \langle -1 \rangle$.

Нека G е група, $a \in G$, $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} \leq G$. Ако за $\forall m, n \in \mathbb{Z}$, такива че $m \neq n$, имаме че $a^m \neq a^n$, то $\langle a \rangle$ е безкрайна група.

Нека сега разгледаме случая, когато $\exists m, n \in \mathbb{Z}$, такива че $m \neq n$, но $a^n = a^m$. Без ограничение на общността считаме, че $m < n$ и след умножение на двете страни с a^{-m} получаваме, че $a^{n-m} = e$ (единичният елемент на G) и $n - m \in \mathbb{N}$. Нека r е най-малкото естествено число, за което $a^r = e$ и разгледаме елементите

$$(*) \quad a^0 = e, a, a^2, \ldots, a^{r-1}.$$

Тези елементи са всичките различни. Наистина, ако допуснем, че $\exists i, j$, такива че $i \neq j$ и $1 \leq i < j \leq r-1$, за които $a^i = a^j$, то след умножение на двете страни с a^{-i} получаваме, че $a^{j-i} = e$ и $j - i < r$, което противоречи на избора на r. Нещо повече, всеки елемент от $\langle a \rangle$ съвпада с някой от елементите $(*)$. Наистина, нека $a^n \in \langle a \rangle$ за $n \in \mathbb{Z}$. Тогава според теоремата за деление с частно $t \in \mathbb{Z}$ и остатък $s \in \mathbb{Z}$ имаме, че $n = rt + s$ и $0 \leq s < r$. Тогава $a^n = a^{rt+s} = a^{rt}a^s = (a^r)^t a^s = e^t a^s = ea^s = a^s$ за някое $0 \leq s \leq r-1$ или с други думи за произволен елемент $a^n \in \langle a \rangle$ доказахме, че е един от елементите $(*)$. По този начин $\langle a \rangle = \{a^0, a, a^2, \ldots, a^{r-n}\}$ е циклична група от ред $|\langle a \rangle| = r$, където r е най-малкото естествено число, такова че $a^r = e$.

В случая когато $\nexists n \in \mathbb{N}$, такова че $a^n = e$, казваме, че a е *елемент от безкраен ред* и означаваме $|a| = \infty$. Ако $\exists n \in \mathbb{N}$, такова че $a^n = e$ и r е най-малкото естествено число с това свойство, то казваме че a е *елемент от ред* r и пишем $|a| = r$.

Пример:

Да разгледаме множеството $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$, което е група спрямо умножението с единичен елемент 1. За $1 \in \mathbb{C}^*$ имаме, че $1^1 = 1$ и следователно $|1| = 1$; за $-1 \in \mathbb{C}^*$ имаме, че $(-1)^2 = 1$ и следователно $|-1| = 2$; за $i \in \mathbb{C}^*$ имаме, че $i^4 = 1$ и следователно $|i| = 4$; за $3 \in \mathbb{C}^*$ не съществува естествено число n, такова че $3^n = 1$ и следователно $|3| = \infty$.

С разсъжденията си дотук доказахме

Твърдение 1. *За всеки елемент $a \in G$, редът на цикличната подгрупа $\langle a \rangle \leq G$ е равен на реда на елемента a. (Т.е. $|\langle a \rangle| = |a|$.)*

Твърдение 2. *Нека G е група, $a \in G$ и $|a| = r$ за $r \in \mathbb{N}$. Ако $m \in \mathbb{Z}$, то е изпълнено $a^m = \Leftrightarrow r$ дели m.*

Доказателство. Необходимост: нека $m \in \mathbb{Z}$ е такова число, че $a^m = e$. Делим m на r с частно $t \in \mathbb{Z}$ и остатък $s \in \mathbb{Z}$, такъв че $0 \leq s < r$. Тогава имаме, $a^m = a^{tr+s} = a^{tr}a^s = (a^r)^t a^s = ea^s = a^s$. Ако допуснем, че $s \neq 0$, то $s \in \mathbb{N}$, $s < r$ и $a^s = e$, но това противоречи на дефиницията на ред r на елемента a. Следователно $s = 0$, което означава, че $m = tr$ и $r \mid m$.

Достатъчност: Нека $r \mid m$. Това означава, че съществува $t \in \mathbb{Z}$, такова че $m = rt$. В равенството $a^r = e$ вдигаме двете страни на степен t и получаваме $a^{rt} = a^m = e$. □

Следващата теорема класифицира цикличните групи.

Теорема 1. *(i) Всяка безкрайна циклична група е изоморфна на групата $\mathbb{Z}$. (С други думи $\mathbb{Z}$ е единствената безкрайна циклична група, с точност до изоморфизъм.)*

(ii) Всяка крайна циклична група от ред $n \in \mathbb{N}$ е изоморфна на групата $\mathbb{C}_n$. (С други думи, при дадено $n \in \mathbb{N}$ групата $\mathbb{C}_n$ е единствената крайна циклична група, с точност до изоморфизъм.)

Доказателство. (i) Нека G е безкрайна циклична група. Това означава, че $\exists a \in G : G = \langle a \rangle = \{\dots, a^{-2}, a^{-1}, a^0 = e, a^1, a^2, \dots\}$ и всеки елемент на G има вида a^n с еднозначно определено цяло число $n \in \mathbb{Z}$, т.к. знаем, че в безкайните циклични групи от $m, n \in \mathbb{Z}, m \neq n$ следва $a^m \neq a^n$. От друга страна $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$. Разглеждаме изображението

$$\varphi : G \longrightarrow \mathbb{Z},$$

зададено с $\varphi(a^n) = n$. Тогава за $m, n \in \mathbb{Z}$ имаме, че $a^m, a^n \in G$ и $\varphi(a^m a^n) = \varphi(a^{m+n}) = m + n = \varphi(a^m) + \varphi(a^n)$. С това φ е хомоморфизъм на групи. Лесно се вижда и че φ е биекция. Наистина, ако $n \in \mathbb{Z}$, то $a^n \in G$ и $\varphi(a^n) = n$. Така φ е сюрекция[2]. Ако $a^m, a^n \in G$ са такива, че $a^m \neq a^n$, то следва и че $m \neq n$, което означава, че $\varphi(a^m) \neq \varphi(a^n)$. По този начин φ е инекция[3], а оттам и биекция. С това доказахме, че φ е изоморфизъм, което значи и че $G \cong \mathbb{Z}$.

(ii) Нека G е циклична група от ред n. Тогава имаме, че

$$G = \langle a \rangle = \left\{a^0 = e, a^1, a^2, \dots, a^{n-1}\right\}.$$

[2]Сюрективните хомоморфизми се наричат още епиморфизми.

[3]Инективните хомоморфизми се наричат още мономорфизми.

От друга страна вече видяхме, че $\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ е пораждащ на групата $\mathbb{C}_n$ и

$$\mathbb{C}_n = \left\{\omega^0 = 1, \omega, \omega^2, \ldots, \omega^{n-1}\right\}.$$

Разглеждаме изображението

$$\varphi : G \longrightarrow \mathbb{C}_n,$$

зададено с $\varphi(a^k) = \omega^k$ за $k = 0, 1, \ldots, n-1$. Очевидно φ е биекция. Да видим и че φ е хомоморфизъм. За произволни елементи $a^k, a^l \in G$, $0 \leq k, l \leq n-1$ имаме, че $a^k a^l = a^{k+l}$ и ако при деление на $k+l$ на n с частно t и остатък s, $0 \leq s < n$ имаме $k+l = nt+s$, то $a^{k+l} = a^{nt+s} = a^s \in G$. По абсолютно същия начин, т.к. $\omega^n = 1$ имаме и $\omega^{k+l} = \omega^s$. Сега вече може да запишем $\varphi(a^k a^l) = \varphi(a^{k+l}) = \varphi(a^s) = \omega^s = \omega^{k+l} = \omega^k\omega^l = \varphi(a^k)\varphi(a^l)$. Така φ е хомоморфизъм, а оттам и изоморфизъм на групи и $G \cong \mathbb{C}_n$. $\square$

След като вече класифицирахме двата вида циклични групи е време да разгледаме и подгрупите, които те притежават.

Теорема 2. *(i) Ако G е циклична група и $H \leq G$, то H също е циклична група.*

(ii) Подгрупите на $\mathbb{Z}$ се изчерпват с $m\mathbb{Z}$ за $m = 0, 1, 2, \ldots$

(iii) Подгрупите на $\mathbb{C}_n$ се изчерпват с $\mathbb{C}_d$, където $d \in \mathbb{N} : d \mid n$.

Доказателство. (i) Нека $G = \langle a\rangle$ е произволна циклична група, а $H \leq G$. Ако $H = \{e\}$, то очевидно H е циклична. Да разгледаме нетривиалния случай $H \neq \{e\}$. Тогава $\exists x \in H : x \neq e$. Т.к. $x \in H$ и $H \subseteq G$, то разглеждайки x като елемент на G имаме, че $\exists s \in \mathbb{Z}\backslash\{0\} : x = a^s$. Но $H \leq G$ и следователно $x^{-1} \in H$, което означава, че $a^{-s} \in H$ като $s \in \mathbb{N}$ или $-s \in \mathbb{N}$. Изборame m да бъде най-малкото естествено число, такова че $a^m \in H$. Тогава очевидно $\langle a^m\rangle \subseteq H$, т.е. цикличната група, породена от a^m е подмножество на H. За произволен елемент $h \in H$ имаме, че $h = a^t, t \in \mathbb{Z}$ и делим t на m с частно $u \in \mathbb{Z}$ и остатък $r \in \mathbb{Z} : 0 \leq r < m$. Тогава $h = a^t = a^{um+r} = (a^m)^u a^r$. Ако допуснем, че $r \neq 0$, то имаме, че $h \in H, (a^m)^u \in H$, откъдето ще следва, че трябва и $a^r \in H$ за $r \in \mathbb{N}, r < m$, но това е противоречеие, т.к. вече бяхме избрали m като най-малкото естествено число, за което $a^m \in H$. Следователно $h = a^t = (a^m)^u \in \langle a^m\rangle$. По този начин $H \subseteq \langle a^m\rangle$, откъдето следва и че $H = \langle a^m\rangle$ и H е циклична група.

(ii) $\mathbb{Z} = \langle 1 \rangle$. Нека $H \leq \mathbb{Z}$. Ако $H = \{0\}$, то нещата са ясни. Нека $H \neq \{0\}$. Тогава според (i) имаме, че $H = \langle m1 \rangle$, където m е най-малкото естествно число, за което $m1 \in H$. Това означава точно, че $H = \langle m \rangle = m\mathbb{Z}$.

(iii) Да разгледаме $\mathbb{C}_n, n \in \mathbb{N}$. Тогава $\mathbb{C}_n = \langle \omega \rangle = \{\omega^0 = 1, \omega, \omega^2, \ldots, \omega^{n-1}\}$. Нека $H \leq \mathbb{C}_n$. Ако $H = \{1\}$, то $H = \mathbb{C}_1$ и $1 \mid n$, с което нещата са доказани. Нека $H \neq \{1\}$. От (i) iимаме, че $H = \langle \omega^m \rangle$, където m е най-малкото естествено число, за което $\omega^m \in H$. Делим n на m с частно $d \in \mathbb{Z}$ и остатък $r \in \mathbb{Z}$, $0 \leq r < m$. Тогава $1 = \omega^n \in H$, т.е. $(\omega^m)^d \omega^r \in H$. От $\omega^m \in H$ следва, че $(\omega^m)^d \in H$ и следователно трябва и $\omega^r \in H$. Както и преди, допускането $r \neq 0$ води до противоречие с избора на m и следователно $r = 0$, а $n = md$, т.е. $d \mid n$ и знаем, че $\mathbb{C}_d \leq \mathbb{C}_n$. Остава да докажем, че $\mathbb{C}_d = \langle \omega^m \rangle$. Първо, $(\omega^m)^d = \omega^{md} = \omega^n = 1$ и следователно $\omega^m \in \mathbb{C}_d$, откъдето пък следва, че $\langle \omega^m \rangle \subseteq \mathbb{C}_d$. Второ, ще докажем, че $|\langle \omega^m \rangle| = d = |\mathbb{C}_d|$, откъдето $\langle \omega^m \rangle \subseteq \mathbb{C}_d$, но имат равен брой елементи и ще следва, че $\langle \omega^m \rangle = \mathbb{C}_d$. Наистина, знаем че редът на цикличната група $|\langle \omega^m \rangle|$ е равен на редът на пораждащия елемент $|\omega^m|$. Да видим какъв е реда на ω^m. Ако $i \in \mathbb{Z}, 1 \leq i < d$ и допуснем, че $(\omega^m)^i = 1$, то $mi < md = n$ и се оказва, че ω е от ред $mi < n$, което е противоречие с факта, че ω е n-ти комплексен корен на единицата. Т.к. вече видяхме, че $(\omega^m)^d = \omega^n = 1$ следва, че d е първото естествено число, за което $(\omega^m)^d = 1$, което означава, че $|\omega^m| = d$. Оттук следва и че $|\langle \omega^m \rangle| = d$, с което показахме, че $|\langle \omega^m \rangle| = |\mathbb{C}_d|$. И така, $H = \langle \omega^m \rangle = \mathbb{C}_d$ за $d \mid n$. $\square$

Пример:
Подгрупите на групата $\mathbb{C}_{12}$ са $\mathbb{C}_1, \mathbb{C}_2, \mathbb{C}_3, \mathbb{C}_4, \mathbb{C}_6, \mathbb{C}_{12}$.