ВА! Каспарян

Ред на елемент

Деф Нека G е гр., $g \in G$, $m \in \mathbb{Z}$. Тогава $g^m = \begin{cases} e & \text{за } m = 0 \\ \underbrace{g \cdot \ldots \cdot g}_{|m|} & \text{за } m \neq 0 \end{cases}$ (e - неутр. ел.)

За $m \neq 0$, $\operatorname{sign}(m) = \begin{cases} 1 & \text{за } m > 0 \\ -1 & \text{за } m < 0 \end{cases}$, $m = \operatorname{sign}(m) \cdot |m|$

Лема Нека G е гр., $g \in G$, $m, n \in \mathbb{Z}$, то $g^m g^n = g^{m+n}$

Док Нека $m = 0$, то $g^m g^n = g^0 g^n = e g^n = g^n = g^{0+n}$. Аналогично за $n = 0$. Остук нагледно $m \neq 0$ и $n \neq 0$.

Нека $\operatorname{sign}(m) = \operatorname{sign}(n) = \varepsilon$, то $m + n = \varepsilon|m| + \varepsilon|n| = \varepsilon|m+n|$. Сега $g^m g^n = \underbrace{g^\varepsilon \cdot \ldots \cdot g^\varepsilon}_{|m|} \underbrace{g^\varepsilon \cdot \ldots \cdot g^\varepsilon}_{|n|} = \underbrace{g^\varepsilon \cdot \ldots \cdot g^\varepsilon}_{|m|+|n|} = g^{\varepsilon(|m|+|n|)} = g^{m+n}$

Нека $|m| \geq |n|$, $\operatorname{sign}(m) = \varepsilon$, $\operatorname{sign}(n) = -\varepsilon$

т.е. $m + n = \varepsilon|m| - \varepsilon|n| = \varepsilon(|m| - |n|)$.

Тогава $g^m g^n = \underbrace{g^\varepsilon \cdot \ldots \cdot g^\varepsilon}_{|m|} \underbrace{g^{-\varepsilon} \cdot \ldots \cdot g^{-\varepsilon}}_{|n|} = \underbrace{g^\varepsilon \cdot \ldots \cdot g^\varepsilon}_{|m|-|n|} = g^{\varepsilon(|m|-|n|)} = g^{m+n}$

Тук използваме че $g^{\varepsilon - \varepsilon} = e$. Т.е. $g g^{-1} = e$ и $g^{-1} g = e$. □

Лема Нека G е гр., $g \in G$, $m, n \in \mathbb{Z}$ то $(g^m)^n = g^{m \cdot n}$

Док

1 сл Ако $n=0$, то $(g^m)^n = (g^m)^0 = e = g^{0 \cdot m} = g^{m \cdot n}$

2 сл За $n \in \mathbb{N}$, $(g^m)^n = \underbrace{g^m \cdot \ldots \cdot g^m}_{n} = g^{\underbrace{m+\ldots+m}_{n}} = g^{m \cdot n}$

3 сл Ако $n \in \mathbb{Z}$, $n < 0$ то $(g^m)^n = (g^m)^{-|n|} =$

$$\underbrace{(g^m)^{-1} \cdot \ldots \cdot (g^m)^{-1}}_{|n|} = \underbrace{g^{-m} \cdot \ldots \cdot g^{-m}}_{|n|} = g^{\frac{(-m)+\ldots+(-m)}{|n|}} = g^{(-m)|n|} = g^{m(-|n|)} = g^{mn}$$

Тук използвахме че $(g^m)^{-1} = g^{-m}$ защото $(g^m)^{-1}$ и g^{-m} са решения на $g^m \cdot x = e \in G$ и това уравнение има единствено решение в G

Нека G е гр, $g \in G$, $\exists z \in \mathbb{Z} \setminus \{0\}$ с $g^z = e$. Тогава и $g^{-z} = e$, така че $\exists m \in \mathbb{N}$ с $g^m = e$

Опр
Ако $g \in G$ е гр, $g \in G$ и $g^z = e$ за някое $z \in \mathbb{Z} \setminus \{0\}$ то ще естествено с усл-то $g^r = e$ е нарича ред на g
Казваме че $g \in G$ има ∞ ред ако $g^z \neq e$ за $\forall z \in \mathbb{Z} \setminus \{0\}$
Твърдим че елементът g на гр G е ∞ ред $\Leftrightarrow g^m \neq g^n$ за $\forall m, n \in \mathbb{Z}$, $m \neq n$. Наистина, ако $g \in G$ е ∞ ред и допуснем че $g^m = g^n$ за $m, n \in \mathbb{Z}$, $m = n$, без ограничение приемаме $m \geq n$. Тогава

$f(n) = g^n = e$

$g^{m-n} = g^m g^{-n} = g^n g^{-n} \Rightarrow$ следователно $g^{-n} = g^{-n}$. Откъдето $g^{m-n} = e$ за $m-n \in \mathbb{N}$ с $\mathbb{Z} \setminus \{0\}$ противоречи на предположението, че e от краен ред

Ако $g^m \neq g^n$ за $\forall m, n \in \mathbb{Z}$, $m \neq n$ то в частност за $m = 0$ имаме че $g^{m-n} \neq g^0 \neq e$ за $\forall n \in \mathbb{Z} \setminus \{0\}$ $\Rightarrow$ g е от безкраен ред

Следователно $\forall$ елемент g на крайна гр G е от краен ред

Ако $|G| < \infty$ то G може да има много елементи от кр ред, така и елементи от ∞ ред. Например $\sqrt{-1} = i \in (\mathbb{C}^*, \cdot)$ е от ред 4, а $2 \in (\mathbb{C}^*, \cdot)$ е от безкраен ред

Лема

Нека G е гр, $g \in G$ е елемент от ред $r \in \mathbb{N}$. В този случай $g^m = e$ за $m \in \mathbb{Z} \Leftrightarrow$, когато $r | m$ (т.е. m се дели на r)

Док $\Rightarrow$

Ако $g^m = e$, делим $m = rq + s$ на r с частно $q \in \mathbb{Z}$ и остатък $s \in \mathbb{N}$ $0 \leq s \leq r-1$. Тогава $e = g^m = g^{rq+s} = g^{rq} g^s = (g^r)^q g^s = e^q g^s = e g^s = g^s$. Допускането $s \neq 0$ води до противоречие с избора на r като минимално естествено с $g^r = e$ и показва че $s = 0$. Следователно $r | m$

2)

Ако $m = 2q$ за някое $q \in \mathbb{Z}$, то $g^m = g^{2q} = (g^2)^q = e^q = e$

Обратно

Нека G е гр., $g \in G$ е елемент от ред 2, и $k \in \mathbb{N}$ и $(2,k) \in \mathbb{N}$ е НОД на 2 и k. Тогава g^k е от ред $2/(2,k)$

Дом

От $g^2 = e \Rightarrow (g^k)^2 = g^{2k} = (g^2)^k = e^k = e$

и елемента $g^k \in G$ е от краен ред s. Сега

Нетрудно $e = (g^k)^s = g^{ks} = g^{(k,2)k_1 s}$ за $k_1 = k/(k,2)$

Отчуи $2 = 2_1/(2,k)$ дели $(k,2)k_1 s$. С други думи НОД на $(k,2)k_1 s = q 2_1 (k,2)$ за някое $q \in \mathbb{Z}$ тогава от $(k,2) \neq 0$ следва $2 k_1 s = q 2_1$. Отчуе $2_1 / k_1 s$ и $(2_1, k_1) = 1$ следователно $2_1 / s$ От друга страна $(g^k)^{2_1} = g^{k 2_1} = g^{k_1 (2,k) 2_1} = (g^{2 k_1})^{2_1} = e^{k_1} = e$ тъй като ред g дели $2_1 k_1$ от $2_1 / 2$ и $s / 2_1$ за $s, 2_1 \in \mathbb{N}$ следва $s = 2_1 = 2/(2,k)$

Циклични групи

Нека G е гр. $g \in G$ тогава подмножеството $\langle g \rangle \overset{def}{:=} \{ g^m / m \in \mathbb{Z} \}$ $\subseteq G$ е ПГ на G, което се нарича циклична ПГ породена от g. Ясно, за $\forall m, n \in \mathbb{Z}$

имаме $g^m(g^n)^{-1} = g^m g^{-n} = g^{m-n} \in \langle g \rangle$ и
това множество е $\neq \emptyset$ на G ($\subseteq G$)
Цикличната гр. порядъка g е
абелева, съгласно $gg = g^{m+n} = g^{n+m} = g^n g^m$
Лема
Нека $G \in \mathcal{GR}$, $g \in G$. В такъв случай
$g \in G$ е от краен ред $\Leftrightarrow$ цикличната
група $\langle g \rangle$ е от краен ред и може
да се представи $\langle g \rangle = \{e, g, \dots, g^{r-1}\}$
Док. $\Rightarrow$
Ако $g \in G$ е от ред r, то за $m \in \mathbb{Z}$ делим
$m = rq + s$ за $r \in$ частно $q \in \mathbb{Z}$ и остатък
$s \in \mathbb{Z}$. $0 \leq s \leq r-1$ Представяме
$g^m = g^{rq+s} = (g^r)^q g^s = e^q g^s = g^s$ и получаваме
че $\forall m \in \mathbb{Z}$ $\langle g \rangle = \{g^m / m \in \mathbb{Z}\} \subseteq \{g^0 = e, g, \dots, g^{r-1}\}$
но $\{g, \dots, g^{r-1}\} \subseteq \{g^m / m \in \mathbb{Z}\} = \langle g \rangle$ следва
$\langle g \rangle = \{e, g, \dots, g^{r-1}\}$
Твърдим че $e = g^0, g, \dots, g^{r-1}$ са
различни помежду си, защото от
$g^i = g^j$ за $i < j < r-1 \Rightarrow e = g^{j-i} g^{-i} = g^{j-i}$
за $j - i \in \mathbb{N}$, $j - i \leq (r-1) - 0 = r - 1 < r$
Т.е. противоречие на предпол. $\Rightarrow$
че $g \in G$ е от ред r показахме че
$\forall t \in \langle g \rangle$ е от ред $\leq r$ или g е от ред r
Нека $\forall t \in \langle g \rangle$ е от ред $\leq r$. Тогава
$g \in G$ е от ред $\leq r$, защото за
$\forall g \in G$ от ∞ ред имаме цикл.
подгрупа на множеството
$\langle g \rangle = \{g^m / m \in \mathbb{Z}\} \supseteq \mathbb{Z}$

ВВ

Съгласно дом-то, ако ε от ред n тогава ЦГ $\langle \varepsilon \rangle$ от ред s - отгук и $s = n$ което $\langle \varepsilon \rangle = \{\varepsilon^0 = \varepsilon^{s-1}\}$

Примери за ЦГ

1) $(\mathbb{Z}, +) = \langle 1 \rangle = \mathbb{Z}$ - защото в адитивна група $\mathbb{Z}$ числа $\mathbb{Z} = \{n \cdot 1 \mid n \in \mathbb{Z}\} = \{n(-1) \mid n \in \mathbb{Z}\}$ и $\mathbb{Z} \in$ ЦГ

2) За $\forall n \in \mathbb{N}$, адитивна $\mathbb{Z}_n = \{\varepsilon (\mathrm{mod}\, n) \mid 0 \le \varepsilon \le n-1\}$ на остатъците при деление с n е ЦГ от ред n относно събирането

$\varepsilon (\mathrm{mod}\, n) + s (\mathrm{mod}\, n) = (\varepsilon + s) (\mathrm{mod}\, n)$

$(\mathbb{Z}_n, +) \in$ гр:

1) асоциативност

$[\varepsilon (\mathrm{mod}\, n) + s (\mathrm{mod}\, n)] + t (\mathrm{mod}\, n) =$

$= ((\varepsilon + s) + t) (\mathrm{mod}\, n) = [\varepsilon + (s + t)] (\mathrm{mod}\, n)$

$= \varepsilon (\mathrm{mod}\, n) + (s + t) (\mathrm{mod}\, n) = \varepsilon (\mathrm{mod}\, n) + [s (\mathrm{mod}\, n) + t (\mathrm{mod}\, n)]$

2) $\exists$ неутр. елемент $0 (\mathrm{mod}\, n)$

3) $\forall \varepsilon (\mathrm{mod}\, n)$ има противоположен $(-\varepsilon) (\mathrm{mod}\, n)$

$\mathbb{Z}_n = \{\varepsilon \cdot 1 (\mathrm{mod}\, n) \mid \varepsilon \in \mathbb{Z}\} = \{\varepsilon (1 \mathrm{mod}\, n)) \mid 0 \le \varepsilon \le n-1\}$

$\mathbb{Z}_n \in$ ЦГ от ред $n \in \mathbb{N}$

$\mathbb{Z}_n = \langle 1 (\mathrm{mod}\, n) \rangle$

Твърдение

Всяка факторизация на ЦГ-ца е ЦГ $\langle \bar{g} \rangle$ е изоморфна на

адитивната гр на целите числа
(ii) е ЦГ от ред $n \in \mathbb{N}$ и изоморфна
мултипликативната гр на корените
$(\mathbb{Z}_n, +)$
от 1
Ако $\langle g \rangle$ е ЦГ то изоморф-то
$f_0 : \mathbb{Z} \to \langle g \rangle$, $f_0(m) = g^m$ за $\forall m \in \mathbb{Z}$ е
единствено определено едно
от ф-ро. Об
$f_0(m+n) = g^{m+n} = g^m g^n = f_0(m) f_0(n)$
за $\forall m, n \in \mathbb{Z}$. Показва се
f_0 е хомоморфизъм от тази
и изоморфизъм на групи
(vi) Ако $\langle g \rangle$ е ЦГ от ред
то $f_n : \mathbb{Z}_n \to \{e, g, \dots, g^{n-1}\}$,
$f_n(a \pmod n) := g^a$ за $\forall a \in \mathbb{Z}$ е
коректно зададено изобр-е
по-точно ако $a_1 (\mathrm{mod}\, n) = a (\mathrm{mod}\, n)$
то $a_1 - a = nq$ за $q \in \mathbb{Z}$ и $g^{a_1} = g^{nq+a}$
$= g^{nq} g^a = e g^a = g^a$ защото g е от ред n
Освен тва f_n е единствено определено
защото за $\forall \bar{c} \in \mathbb{Z}_n$ $0 \le c \le n-1$ $\exists!$
остатък $c (\mathrm{mod}\, n) \in \mathbb{Z}_n$ с
$f_n(c (\mathrm{mod}\, n)) = g^c$. Тъй като $f_n : \langle g \rangle \to$
$\mathbb{Z}_n$, $f_n^{-1}(g^c) = c (\mathrm{mod}\, n)$ е коректно
зададено изображение. Освен
това $f_n(c (\mathrm{mod}\, n) + s (\mathrm{mod}\, n)) = f_n(c+s)$
$(\mathrm{mod}\, n)) = g^{c+s} = g^c g^s = f_n(c (\mathrm{mod}\, n)) f_n(s \dots)$
следва че f_n е хом-зъм от групи и
изоморф-зъм на групи $\square$

Тв-е

Н ПГ-а Н на ЦГ $G = \langle g \rangle \in$ Ц-а
То-тогда $H = \{e\}$ или $H = \langle g^m \rangle$ за
минималното $m \in \mathbb{N}$ с усл-то
$g^m \in H$

Док

Ако $\exists z \in \mathbb{Z} \setminus \{0\}$ с усл-то $g^z \in H$, то
$g^{-z} = (g^z)^{-1} \in H$ и $\exists t \in \mathbb{N}$ с $g^t \in H$
Нека $m \in \mathbb{N}$ е мин-то сбс $g^m \in H$
Тогава за ЦГ $\langle g^m \rangle = \{(g^m)^s = g^{ms} | s \in \mathbb{Z}\} \in H$
т.к $g^{-m} \in H$ и за $\forall n \in \mathbb{N}$ имаме
$(g^{-m})^n = g^{-mn} \cdot g^{-mn} \in H \leq G = \langle g \rangle$. За
произволното n е вярно горното
$g^{\ell} \in H$ за $\forall \ell \in \mathbb{Z}$. Сега делението
$\ell = mq + r$ на $m \in \mathbb{N}$ с частно
$q \in \mathbb{Z}$ и ост $r \in \mathbb{Z}$ $0 \leq r \leq m-1$
Тогава $r = \ell - mq$, откъдето $g^r = g^{\ell - mq} = g^{\ell}(g^m)^{-q}$
$\in H$ т.к $g^{\ell} \in H$ и $(g^m)^{-q} \in \langle g^m \rangle \leq H$
Допуск-ме $r \neq 0$ води до противоречие
с минималността на $m \in \mathbb{N}$ с $g^m \in H$
сл

Ако нямаме $\langle g \rangle \in$ ЦГ пр-ба ред
и $m \in \mathbb{N}$ е мин-то с усл-то $g^m \in H$
за $H \leq \langle g \rangle$, то м/к $H = \langle g^m \rangle$ е
ред $|H| = \frac{n}{m} = k$

За $\forall k \in \mathbb{N}$, $k | n$, $n \in \mathbb{N}$, $\exists!$ на ПГ
H на ЦГ $Z_n \cong \langle g \rangle = \{g^0 = e, g, \ldots, g^{n-1}\}$ с
ред $|H| = k$. По-тогава $H = \langle g^{\frac{n}{k}} \rangle$