Групи - определение, примери, основни свойства.

Определение 1. *Нека G е непразно множество. Всяко изображение $G \times G \to G$ се нарича бинарна операция в G.*

Ако F е числово поле, то събирането $F \times F \to F$, $(a, b) \mapsto a + b$ и умножението $F \times F \to F$, $(a, b) \mapsto ab$ в F са бинарни операции.

Определение 2. *Непразно множество G е група, ако в него е зададена бинарна операция $G \times G \to G$ със свойствата:*

(i) асоциативност - $(ab)c = a(bc)$ за всички $a, b, c \in G$;

(ii) съществуване на неутрален елемент $e \in G$, така че $ae = ea = a$ за всяко $a \in G$;

(iii) всеки елемент $a \in G$ има обратен $a^{-1} \in G$, така че $aa^{-1} = a^{-1}a = e$ за някой неутрален елемент e.

Определение 3. *Група G е абелева, ако $ab = ba$ за всички елементи $a, b \in G$.*

Пример за абелева група е адитивната група $(\mathbb{Z}, +)$ на целите числа. Тук използваме асоциативността и комутативността на събирането на цели числа. Неутрален елемент на $(\mathbb{Z}, +)$ е числото $0 \in \mathbb{Z}$. Обратният на $a \in \mathbb{Z}$ е $-a \in \mathbb{Z}$.

Ако F е числово поле, то абелевата група $(F, +)$ се нарича адитивна група на F, а абелевата група $(F^* := F \setminus \{0\}, .)$ е известна като мултипликативна група на F. За да обясним защо $(F, +)$ и $(F^*, .)$ са групи да отбележим, че събирането и умножението в числово поле F са асоциативни и комутативни бинарни операции. Неутрален елемент на F е $0 \in F$ и всеки елемент $a \in F$ има обратен $-a \in F$. Неутрален елемент на $(F^*, .)$ е 1, а всяко $a \in F^* = F \setminus \{0\}$ има обратен $a^{-1} \in F$.

Ако V е линейно пространство над числово поле F, то $(V, +)$ е абелева група, която се нарича адитивна група на V. Тук използваме асоциативността и комутативността на събирането на вектори във V, наличието на нулев вектор $\overrightarrow{\mathcal{O}} \in V$, така че $a + \overrightarrow{\mathcal{O}} = a$ за всяко $a \in V$ и наличието на противоположен $-a \in V$ за произволен вектор $a \in V$, изпълняващ равенството $a + (-a) = \overrightarrow{\mathcal{O}}$.

Ако F е числово поле и $n \in \mathbb{N}$ е естествено число, то множеството

$$\mathrm{GL}(n, F) = \{A \in M_{n \times n}(F) \mid \det(A) \neq 0\}$$

на неособените матрици от ред n е неабелева група относно обичайното умножение на матрици, която се нарича обща линейна група от степен n над F. Тук използваме асоциативността на умножението на матрици, наличието на единична матрица $E_n \in M_{n \times n}(F)$ с $AE_n = E_n A = A$ за всяко $A \in \mathrm{GL}(n, F)$ и съществуването на обратна матрица $A^{-1} \in \mathrm{GL}(n, F)$ за всяко $A \in \mathrm{GL}(n, F)$, изпълняваща равенствата $AA^{-1} = A^{-1}A = E_n$. Съществуването на матрици

$$A = \begin{pmatrix} 1 & 2 & \mathbb{O}_{1 \times (n-2)} \\ 3 & 4 & \mathbb{O}_{1 \times (n-2)} \\ \mathbb{O}_{(n-2) \times 1} & \mathbb{O}_{(n-2) \times 1} & E_{n-2} \end{pmatrix}, \quad B = \begin{pmatrix} 5 & 6 & \mathbb{O}_{1 \times (n-2)} \\ 7 & 8 & \mathbb{O}_{1 \times (n-2)} \\ \mathbb{O}_{(n-2) \times 1} & \mathbb{O}_{(n-2) \times 1} & E_{n-2} \end{pmatrix}$$

от $\mathrm{GL}(n,F)$ с произведения

$$AB = \begin{pmatrix} 19 & 22 & \mathbb{O}_{1\times(n-2)} \\ 43 & 50 & \mathbb{O}_{1\times(n-2)} \\ \mathbb{O}_{(n-2)\times 1} & \mathbb{O}_{(n-2)\times 1} & E_{n-2} \end{pmatrix} \neq \begin{pmatrix} 23 & 34 & \mathbb{O}_{1\times(n-2)} \\ 31 & 46 & \mathbb{O}_{1\times(n-2)} \\ \mathbb{O}_{(n-2)\times 1} & \mathbb{O}_{(n-2)\times 1} & E_{n-2} \end{pmatrix} = BA$$

показва, че групата $\mathrm{GL}(n,F)$ не е абелева за $n \geq 2$. Да обърнем внимание, че $\mathrm{GL}(1,F) = (F^*,.)$ съвпада с мултипликативната група на F и е абелева.

Нека M е множество, а $f : M \to M$, $g : M \to M$ и $h : M \to M$ са изображения на M в себе си. Тогава $gf : M \to M$, $(gf)(x) = g(f(x))$ за всяко $x \in M$ се нарича произведение на f и g. Непосредствено се проверява, че $h(gf) = (hg)f$, т.е. произведението на изображения на M е асоциативно. Множесттвото $\mathrm{Sym}(M)$ на взаимно-еднозначките изображения $f : M \to M$ е група относно умножението, чийто неутрален елемент е тъждественото изображение $\mathrm{Id}_M : M \to M$, $\mathrm{Id}_M(x) = x$, $\forall x \in M$. Казваме, че $\mathrm{Sym}(M)$ е симетричната група на M.

Ако броят на елементите на M е $n \in \mathbb{N}$, то $\mathrm{Sum}(M)$ се нарича симетрична група от степен n и се бележи с S_n. Елементите $\sigma \in S_n$ се задават във вида

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

и се определят еднозначно от редицата $\sigma(1), \sigma(2), \dots, \sigma(n)$ на образите. Затова $\sigma \in S_n$ се наричат пермутации. Множеството S_n на пермутациите на числата $1, \dots, n$, $n \geq 3$ е неабелева група относно последователното прилагане на пермутации. За да докажем това е достатъчно да забележим, че

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix} = (1,2) \quad \text{и} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 2 & 1 & 4 & \dots & n \end{pmatrix} = (1,3) \in S_n$$

имат различни произведения

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 1 & 4 & \dots & n \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 1 & 2 & 4 & \dots & n \end{pmatrix} = \sigma\tau$$

в единия и другия ред на множителите. Симетричната група $S_2 = \{\varepsilon, \theta\}$ с

$$\theta = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

е абелева. (Проверете, че $ab = ba$ за всички $a, b \in S_2$, използвайки $\theta^2 = \varepsilon$.)

Определение 4. *Група G е крайна, ако има краен брой елементи. В такъв случай, броят на елементитте $|G|$ в G се нарича ред на G.*

Ясно е, че групата $(\mathbb{Z}, +)$ е безкрайна. Ако F е числово поле, то F е безкрайно, защото съдържа безкрайното поле $\mathbb{Q}$ на рационалните числа и $(F,+)$, $(F^*,.)$ са безкрайни групи. Всяко ненулево линейно пространство V над числово поле F е безкрайна група, защото произволен ненулев вектор $u \in V \setminus \{\mathcal{O}\}$ задава безкрайно подмножество $l_F(u) = \{\lambda u \,|\, \lambda \in F\}$ на V. Ако F е числово поле и $n \in \mathbb{N}$ е естествено число, то общата линейна група $\mathrm{GL}(n,F)$ е безкрайна, защото съдържа безкрайното подмножество

$$\left\{ \begin{pmatrix} \lambda_1 & 0 & \dots & 0 & 0 \\ 0 & \lambda_2 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_{n-1} & 0 \\ 0 & 0 & \dots & 0 & \lambda_n \end{pmatrix} \,\Big|\, \lambda_i \in F^* \right\}.$$

Симетричната група S_n е крайна и от ред $|S_n| = n! = n(n-1)(n-2)\dots 2.1$. По-точно, ако $\sigma \in S_n$, то за $\sigma(1) \in \{1,\dots,n\}$ има n възможности. След избора на $\sigma(1)$ има $n-1$ независими възможности за $\sigma(2) \in \{1,\dots,n\} \setminus \{\sigma(1)\}$. По-нататък, за $\sigma(3) \in \{1,\dots,n\} \setminus \{\sigma(1),\sigma(2)\}$ има $n-2$ независими възможности и т.н.

Твърдение 5. *Нека $G \times G \to G$ е асоциативна бинарна операция в непразно множество G. В такъв случай, G е група относно тази операция тогава и само тогава, когато за произволни $a,b \in G$ уравненията $ax = b$ и $ya = b$ имат единствени решения $x_o = a^{-1}b \in G$, съответно $y_o = ba^{-1} \in G$.*

Доказателство. Нека G е група, $a,b \in G$. Тогава $a(a^{-1}b) = (aa^{-1})b = eb = b$ показва, че $x_o = a^{-1}b \in G$ е решение на $ax = b$. Ако $x_1 \in G$ е решение на $ax = b$, то лявото почленно умножение на $b = ax_1$ с $a^{-1} \in G$ дава $x_o = a^{-1}b = a^{-1}(ax_1) = (a^{-1}a)x_1 = ex_1 = x_1$ и доказва единствеността на решението x_o на $ax = b$. Аналогично, от $(ba^{-1})a = b(a^{-1}a) = be = b$ следва, че $y_o = ba^{-1} \in G$ е решение на $ya = b$. Ако $y_1 \in G$ е решение на $ya = b$, то чрез дясно почленно умножение на $b = y_1a$ с a^{-1} получаваме $y_o = ba^{-1} = (y_1a)a^{-1} = y_1(aa^{-1}) = y_1e = y_1$ и установяваме единствеността на решението $y_o = ba^{-1} \in G$ на $ya = b$.

Да предположим, че за произволни $a,b \in G$ уравненията $ax = b$ и $ya = b$ имат единствени решения $x_o, y_o \in G$. Тогава от $uv_1 = uv_2$ за $u,v_1,v_2 \in G$ следва $v_1 = v_2$, защото уравнението $ux = uv_1$ има решения $v_1 \in G$ и $v_2 \in G$. Аналогично, равенството $v_1u = v_2u$ за $u,v_1,v_2 \in G$ може "да се съкрати"отдясно на u и да се получи $v_1 = v_2$, защото уравнението $yu = v_1u$ има решения $v_1 \in G$ и $v_2 \in G$.

За да докажем съществуването на неутрален елемент на G относно разглежданата асоциативна операция забелязваме, че всеки елемент $a \in G$ има десен неутрален $r_a \in G$, така че $ar_a = a$. Определяме $r_a \in G$ като единственото решение на $ax = a$ от G. Аналогично, за всяко $c \in G$ уравнението $yc = c$ има единствено решение $l_c \in G$, което е ляв неутрален за c съгласно $l_cc = c$. Умножаваме почленно $ar_a = a$ с $l_cc = c$ и получаваме $ar_al_cc = ac$. След ляво съкращаване на a извеждаме

$$r_al_cc = c. \tag{1}$$

Лявото почленно умножение на $l_cc = c$ с l_c дава $l_c^2c = l_cc = c$. След заместване в (1) получаваме

$$r_al_cc = l_c^2c,$$

което може да се съкрати отдясно на l_cc, за да се получи

$$r_a = l_c \quad \text{за всички} \quad a,c \in G.$$

По този начин установихме съществуването на универсален неутрален елемент $e = r_a = l_c \in G$, така че $ae = ea = a$ за всяко $a \in G$.

Остава да установим, че всеки елемент $a \in G$ има обратен относно зададената асоциативна операция. За целта използваме, че уравнението $ax = e$ има единствено решение $a_r \in G$, което е десен обратен за a съгласно $aa_r = e$. Аналогично, за всяко $a \in G$ единственото решение $a_l \in G$ на $ya = e$ е ляв обратен на a, защото $a_la = e$. Използвайки асоциативността на зададената операция, извеждаме

$$a_r = ea_r = (a_la)a_r = a_l(aa_r) = a_le = a_l$$

и доказваме съществуването на обратен елемент $a^{-1} = a_r = a_l \in G$ на $a \in G$ с $aa^{-1} = a^{-1}a = e$. Това доказва, чв ако G е непразно множество с асоциативна операция, в която уравненията $ax = b$ и $ya = b$ имат единствени решения за всички $a,b \in G$, то G е група относно тази операция.

□

Следствие 6. *Ако G е група, то:*

(i) за произволни $u, v_1, v_2 \in G$ с $uv_1 = uv_2$ следва $v_1 = v_2$;

(ii) за произволни $u, v_1, v_2 \in G$ с $v_1u = v_2u$ следва $v_1 = v_2$;

(iii) неутралният елемент e на G е единствен;

(iv) всеки елемент $a \in G$ има единствен обратен $a^{-1} \in G$;

(v) $(a^{-1})^{-1} = a$ за произволен елемент $a \in G$;

(vi) $(ab)^{-1} = b^{-1}a^{-1}$ за произволни елементи $a, b \in G$.

Доказателство. (i) и (ii) следват от Твърдение NSCAssOperToDefineGroup, възоснова на това, че във всяка група G уравненията $ax = b$ и $ya = b$ имат единствени решения за произволни $a.b \in G$.

(iii) За произволно фиксирано $a \in G$ уравнението $ax = a$ има единствено решение в G. Неутралните елементи $e_1, e_2 \in G$ са негови решения, така че $e_1 = e_2$.

(iv) Обратният елемент $a^{-1} \in G$ на $a \in G$ е единствен като решение на уравнението $ax = e$.

(iv) По определение, $(a^{-1})^{-1} \in G$ е решение на уравнението $a^{-1}x = e$. Съгласно $a^{-1}a = e$, елементът $a \in G$ е негово решение и $(a^{-1})^{-1} = a$.

(vi) Обратният $(ab)^{-1} \in G$ на $ab \in G$ е решение на уравнението $(ab)x = e$. От $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = (ae)a^{-1} = aa^{-1} = e$ следва, че $b^{-1}a^{-1} \in G$ е решение на $(ab)x = e$, откъдето $(ab)^{-1} = b^{-1}a^{-1}$.

□

Определение 7. *Непразно подмножество H на група G е подгрупа, ако за произволни $a, b \in G$ е в сила $ab, a^{-1} \in H$. Бележим $H \leq G$.*

В частност, неутралният елемент $e = aa^{-1} \in H$ принадлежи на произволна подгрупа H на G. Ако H е подгрупа на група G, то груповата операция $G \times G \to G$ в G се ограничава до бинарна операция $H \times H \to H$ в H. Асоциативността на $G \times G \to G$ се наследява от $H \times H \to H$. Неутралният елемент $e \in G$ принадлежи на всяка подгрупа H и по определение, обратният a^{-1} на елемент $a \in H$ принадлежи на H. Това доказва, че H е група относно наследената от G операция.

Примери за подгрупи:

Ако G е група с неутрален елемент e, то G и $\{e\}$ са подгрупи на G, съгласно $e.e = e$ и $e^{-1} = e$.

За произволно естествено число n, множеството $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$ на кратните на n цели числа е подгрупа на $(\mathbb{Z}, +)$, защото от $na, nb \in \mathbb{Z}$ следва $na + nb = n(a + b) \in n\mathbb{Z}$ и $-(na) = n(-a) \in n\mathbb{Z}$.

Адитивната група $(\mathbb{Q}, +)$ на полето $\mathbb{Q}$ на рационалните числа е подгрупа на адитивната група $(\mathbb{R}, +)$ на полето на реалните числа, защото сумата на рационални числа е рационално число и противоположното на рационално число е рационално.

Мултипликативната група $(\mathbb{Q}^* = \mathbb{Q}\{0\}, .)$ на полето на рационалните числа е подгрупа на мултипликативната група $(\mathbb{R}^* = \mathbb{R} \setminus \{0\}, .)$ на полето на реалните числа, защото произведението на рационални числа е рационално и реципрочното на ненулево рационално число е рационално.

Ако V е линейно пространство над числово поле F, а W е подпространство на V, то адитивната група $(W, +)$ на W е подгрупа на адитивната група $(V, +)$ на V, защото сумата на вектори от W принадлежи на W и противоположния на вектор от W принадлежи на W.

Ако F е числово поле и $n \in \mathbb{N}$ е естествено число, то множеството

$$\mathrm{SL}(n, F) = \{A \in M_{n\times n}(F) \mid \det(A) = 1\}$$

на матриците с детерминанта 1 е подгрупа на общата линейна група $\mathrm{GL}(n,F)$, защото за произволни $A,B \in \mathrm{SL}(n,F)$ в сила $AB, A^{-1} \in \mathrm{SL}(n,F)$, съгласно $\det(AB) = \det(A)\det(B) = 1$ и $\det(A^{-1}) = \frac{1}{\det(A)} = 1$.

Ако $m < n$ са естествено числа, то множеството

$$S'_m = \{\sigma \in S_n \,|\, \sigma(i) = i, \quad \forall m+1 \leq i \leq n\}$$

на пермутациите на $1,\ldots,n$, оставящи на място $m+1,\ldots,n$ е подгрупа на S_n, защото от $\sigma,\tau \in S'_m$ следва $\tau\sigma, \sigma^{-1} \in S'_m$. Ясно е, че $\tau\sigma(i) = \tau(i) = i$, откъдето $\tau\sigma \in S'_m$. От друга страна, $\sigma^{-1}\sigma = \varepsilon$ дава $\sigma^{-1}(i) = \sigma^{-1}(\sigma(i)) = (\sigma^{-1}\sigma)(i) = \varepsilon(i) = i$ за всяко $m+1 \leq i \leq n$ и доказва, че $\sigma^{-1} \in S'_m$.

Твърдение 8. *Непразно подмножество H на група G е подгрупа тогава и само тогава, когато $ab^{-1} \in H$ за произволни $a,b \in H$.*

Доказателство. Ако H е подгрупа на група G и $a,b \in H$, то $b^{-1} \in H$, откъдето $ab^{-1} \in H$.

Ако за произволни $a,b \in H$ е в сила $ab^{-1} \in H$, то неутралният елемент e на G принадлежи на H, защото за произволно $a \in H$ е в сила $e = aa^{-1} \in H$. Сега за всяко $a \in H$ е изпълнено $a^{-1} = ea^{-1} \in H$. За произволни $a,b \in H$ от $b^{-1} \in H$ получаваме $ab = a(b^{-1})^{-1} \in H$ и доказваме, че H е подгрупа на G.

□

Определение 9. *Изображение $\varphi : G_1 \to G_2$ на група G_1 в група G_2 е хомоморфизъм на групи, ако $\varphi(ab) = \varphi(a)\varphi(b)$ за произволни $a,b \in G_1$. Ако $\mu_i : G_i \times G_i \to G_i$ са груповите операции в G_i, то определението за хомоморфизъм на групи е еквивалентно на равенството на изображения $\varphi\mu_1 = \mu_2(\varphi \times \varphi)$ по протежение на диаграмата*

$$\begin{array}{ccc} G_1 \times G_1 & \xrightarrow{\mu_1} & G_1 \\ \downarrow{\scriptstyle \varphi\times\varphi} & & \downarrow{\scriptstyle \varphi} \\ G_2 \times G_2 & \xrightarrow{\mu_2} & G_2 \end{array} .$$

Това се дължи на равенствата $\varphi\mu_1(a,b) = \varphi(ab)$ и $\mu_2(\varphi\times\varphi)(a,b) = \varphi(a)\varphi(b)$ за всички $a,b \in G_1$.

Твърдение 10. *Ако $\varphi : G_1 \to G_2$ е хомоморфизъм на групи, то:*
(i) $\varphi(e_{G_1}) = e_{G_2}$ за неутралните елементи e_{G_i} на G_i;
(ii) $\varphi(a^{-1}) = \varphi(a)^{-1}$ за произволен елемент $a \in G_1$;
(iii) $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1}$ и $\varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b)$ за произволни елементи $a,b \in G_1$.

Доказателство. (i) За произволен елемент $a \in G_1$, да забележим, че неутралният елемент e_{G_2} на G_2 е единственото решение на уравнението $\varphi(a)x = \varphi(a)$ от G_2. Съгласно

$$\varphi(a)\varphi(e_{G_1}) = \varphi(ae_{G_1}) = \varphi(a),$$

елементът $\varphi(e_{G_1}) \in G_2$ също е решение на това уравнение и $\varphi(e_{G_1}) = e_{G_2}$.

(ii) По определение, $\varphi(a)^{-1} \in G_2$ е единственото решение на уравнението $\varphi(a)x = e_{G_2}$ от G_2. С помощта на (i) пресмятаме, че

$$\varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(e_{G_1}) = e_{G_2},$$

така че $\varphi(a^{-1}) \in G_2$ е също решение на $\varphi(a)x = e_{G_2}$ от G_2 и $\varphi(a^{-1}) = \varphi(a)^{-1}$.

(iii) От определението за хомоморфизъм на групи и (ii) извеждаме, че

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} \quad \text{и} \quad \varphi(a^{-1}b) = \varphi(a^{-1})\varphi(b) = \varphi(a)^{-1}\varphi(b)$$

за произволни $a, b \in G_1$.

□

Определение 11. *Ако $\varphi : G_1 \to G_2$ е хомоморфизъм на групи, то множеството*

$$\ker\varphi := \{a \in G_1 \,|\, \varphi(a) = e_{G_2}\}$$

се нарича ядро на φ, а множеството

$$\mathrm{im}\varphi := \{\varphi(a) \,|\, a \in G_1\}$$

се нарича образ на φ.

Твърдение 12. *Ако $\varphi : G_1 \to G_2$ е хомоморфизъм на групи, то:*

(i) ядрото $\ker(\varphi)$ на φ е подгрупа на G_1;

(ii) образът $\mathrm{im}(\varphi)$ на φ е подгрупа на G_2;

(iii) слоят $\varphi^{-1}(\varphi(a)) := \{b \in G_1 \,|\, \varphi(b) = \varphi(a)\}$ на φ през $a \in G_1$ съвпада с множествата $(\ker\varphi)a := \{xa \,|\, x \in \ker\varphi\}$ и $a(\ker\varphi) = \{ax \,|\, x \in \ker\varphi\}$.

В частност, всички слоеве на хомоморфизъм на групи са изоморфни помежду си.

Доказателство. (i) Ядрото $\ker\varphi$ на φ е подгрупа на G_1, защото за произволни $a, b \in \ker\varphi$ е в сила $ab^{-1} \in \ker\varphi$, съгласно $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = e_{G_2}e_{G_2}^{-1} = e_{G_2}$.

(ii) Образът $\mathrm{im}\varphi$ на φ е подгрупа на G_2, понеже за произволни $\varphi(a), \varphi(b) \in \mathrm{im}\varphi$ с $a, b \in G_1$ е изпълнено $\varphi(a)\varphi(b)^{-1} = \varphi(ab^{-1}) \in \mathrm{im}\varphi$.

(iii) Ако $b \in \varphi^{-1}(\varphi(a)) := \{b \in G_1 \,|\, \varphi(b) = \varphi(a)\}$, то $a^{-1}b, ba^{-1} \in \ker\varphi$, съгласно

$$\varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b) = \varphi(a)^{-1}\varphi(a) = e_{G_2}, \quad \varphi(ba^{-1}) = \varphi(b)\varphi(a)^{-1} = \varphi(a)\varphi(a)^{-1} = e_{G_2}.$$

След ляво и дясно умножение с $a \in G_1$ получаваме $b \in a(\ker\varphi)$, съответно, $b \in (\ker\varphi)a$ и доказваме, че слоят $\varphi^{-1}(\varphi(a))$ на φ над $\varphi(a)$ се съдържа в $a(\ker\varphi)$ и $(\ker\varphi)a$.

За произволен елемент $x \in \ker\varphi$ е в сила

$$\varphi(ax) = \varphi(a)\varphi(x) = \varphi(a)e_{G_2} = \varphi(a) \quad \text{и} \quad \varphi(xa) = \varphi(x)\varphi(a) = e_{G_2}\varphi(a) = \varphi(a).$$

Следователно $a(\ker\varphi) \subseteq \varphi^{-1}(\varphi(a))$, $(\ker\varphi)a \subseteq \varphi^{-1}(\varphi(a))$ и

$$a(\ker\varphi) = \varphi^{-1}(\varphi(a)) = (\ker\varphi)a.$$

□

Определение 13. *Взаимно еднозначните хомоморфизми на групи $\psi : G' \to G''$ се наричат изоморфизми на групи.*

Лема 14. *Ако $\psi : G' \to G''$ е изоморфизъм на групи, то обратното изображение $\psi^{-1} : G'' \to G'$ е хомоморфизъм, а оттам и изоморфизъм на групи.*

Доказателство. Трябва да проверим, че ако $\psi : G' \to G''$ е изоморфизъм на групи, то обратното изображение $\psi^{-1} : G'' \to G'$ изпълнява равенствата $\psi^{-1}(xy) = \psi^{-1}(x)\psi^{-1}(y)$ за произволни елементи $x, y \in G''$. Ако $\psi^{-1}(x) = a \in G'$, $\psi^{-1}(y) = b \in G'$, то $x = \psi(a)$, $y = \psi(b)$ и

$$\psi^{-1}(x)\psi^{-1}(y) = ab = \psi^{-1}\psi(ab) = \psi^{-1}(\psi(a)\psi(b)) = \psi^{-1}(xy),$$

вземайки предвид, че ψ е хомоморфизъм на групи.

□