Глава 1

Въведение.

1.1 Основни понятия.

В тази глава ще изложим основните понятия и твърдения без доказателства. За подробности препоръчваме [2], [1], или кой да е учебник по Висша алгебра.

Дефиниция 1.1.1 ***Група*** *наричаме непразно множеството G с въведена в него бинарна операция $\circ : G \times G \to G$, която притежава (удовлетворява) следните свойства:*

1. *За всеки $g, h, k \in G$: $(g \circ h) \circ k = g \circ (h \circ k)$* ***асоциативност;***
2. *Съществува елемент $e \in G$, такъв че за всяко $g \in G$: $e \circ g = g$ (****ляв единичен елемент****);*
3. *За всяко $g \in G$ съществува елемент $g' \in G$ такъв, че $g' \circ g = e$ (****ляв обратен елемент на*** *g).*

Непосредствени следствия от дефиницията:

1. Левият обратен е и десен обратен, т. е. $g \circ g' = e$;
2. Лявата единица е и дясна единица, т. е. $g \circ e = g$;
3. Единственост на **обратния елемент на** g: За всяко $g \in G$ съществува **единствен** елемент g', такъв че $g' \circ g = g \circ g' = e$
4. Единственост на единичния елемент: Съществува **единствен** елемент $e \in G$, такъв че за всяко $g \in G$ е в сила $g \circ e = e \circ g = g$.

Да отбележим, че "вземането на обратен елемент" задава унарна операция в групата.

Ако за всеки два елемента $a, b \in G$ е изпълнено $a \circ b = b \circ a$ казваме, че групата е ***комутативна или абелева***. При такива групи като знак за бинарната операция много често се използва знакът "+". В този случай се казва, че групата е ***адитивно записана*** или просто ***адитивна***. В адитивен запис "степента" на един елемент (т. е. многократното прилагане на бинарната операция) има вида $m.g \stackrel{\text{def}}{=} \underbrace{g + g + \cdots + g}_{m}$, а

вместо понятието единичен елемент се ползва ***нулев елемент***, 0. Обратният елемент, съответно се нарича ***противоположен елемент*** и бележи с $-g$.
Когато се ползва знакът "." (или някой друг, както в дефиницията по-горе) говорим за ***мултипликативен запис*** (***мултипликативна група***) и при него $g^m \stackrel{\text{def}}{=} \underbrace{g.g.\cdots.g}_{m}$, а единичният елемент се означава често с 1, обратният - с g^{-1}.

Ако групата G се състои от n елемента, т. е. $|G| = n$, казваме, че тя е ***крайна група с ред*** n. Ако G има безброй много елементи казваме, че тя е ***безкрайна група (има безкраен ред)***.

Дефиниция 1.1.2 *Нека G е група. Подмножеството H на G наричаме* ***подгрупа****, ако самото то е група относно бинарната операция в G.*

Твърдение 1.1.3 *Подмножествота $H \subset G$ е подгрупа тогава и само тогава, когато е затворено относно операциите в G, т. е. за всяко $a, b \in G$ е изпълнено $ab \in G$, $a^{-1} \in G$.*

Всяка група има поне две подгрупи, G и $\{e\}$, които се наричат тривиални подгрупи. Подгрупа, различна от G и $\{e\}$ се нарича ***собствена подгрупа***.

Пример 1.1.1 Съвкупността от целите числа $\mathbb{Z}$ (също така $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, съответно) образуват абелева група относно обичайното действие събиране (адитивна група).

Пример 1.1.2 Съвкупността от ненулеви рационални числа $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ ($\mathbb{R}^*, \mathbb{C}^*$ съответно) са група относно умножението (мултипликативни групи).

Пример 1.1.3 Нека Ω е непразно множество. Да разгледаме съвкупността S_Ω от всички биекции на Ω върху себе си. Композицята (последователното прилагане) на две биекции и обратното изображение на биекция са също биекции. Следователно S_Ω е група относно композицията (ще наричаме произведение) на биекции с единичен елемент тъждественото изображение. Тази група ще наричаме ***симетрична група на*** Ω. Много често в литературата се ползва и означението $\mathrm{Sym}(\Omega)$. Ако Ω е крайно множество с n елемента (без ограничение на общност можем да считаме, че $\Omega = \{1, 2, \ldots, n\}$) ще бележим с S_n и ще я наричаме ***симетрична група от степен*** n.

Пример 1.1.4 Съвкупността от обратимите $n \times n$ матрици с елементи от полето $\mathbb{F}$

$$GL(n, \mathbb{F}) \stackrel{\text{def}}{=} \{\mathbf{A} = (a_{ij}) \mid \det \mathbf{A} \neq 0, a_{ij} \in \mathbb{F}\}$$

е група относно умножението на матрици и се нарича ***пълна линейна група***.

Пример 1.1.5 ***Специална линейна група***:

$$SL(n, \mathbb{F}) \stackrel{\text{def}}{=} \{\mathbf{A} \in GL(n, \mathbb{F}) \mid \det \mathbf{A} = 1\}.$$

Дефиниция 1.1.4 *Нека G и G' са групи. Изображение $\varphi : G \to G'$, такова че*

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$$

за всяко $g_1, g_2 \in G$ се нарича ***хомоморфизъм*** *G в G'. Ако φ е биекция, то го наричаме* ***изоморфизъм****. Ако е инекция или сюрекция, говорим за* ***мономорфизъм*** *и* ***епиморфизъм****, съответно. Хомоморфизъм от G в G се нарича* ***ендоморфизъм*** *на G, и изоморфизм на G в G се нарича* ***автоморфизъм*** *на G*

От дефиницията непосредствено следва, че

$$\varphi(1_G) = 1_{G'} \quad \text{и} \quad \varphi(g^{-1}) = \varphi(g)^{-1}$$

В адитивен запис имаме съответно

$$\varphi(0_G) = 0_{G'} \quad \text{и} \quad \varphi(-g) = -\varphi(g).$$

Пример 1.1.6 Нека $P = \{x \in \mathbb{R} \mid x > 0\}$ е групата от всички реални положителни числа (подгрупа на $\mathbb{R}^*$). Изображението

$$\varphi : \left| \begin{array}{ccc} P & \to & \mathbb{R} \\ x & \to & \ln x. \end{array} \right.$$

е пример за изоморфизъм (Докажи!).

Съвкупността от всички автоморфизмите на G е група относно композицията и се нарича ***група от автоморфизмите на*** G. Означава се с $\mathrm{Aut}(G)$. Тя разбира се е подгрупа на S_G.

Две групи G и H наричаме ***изоморфни*** и пишем $G \cong H$, ако съществува изоморфизъм $\varphi : G \to H$. Лесно се проверява, че "$\cong$" е релация на еквивалентност.

Теорема 1.1.5 (Теорема на Кейли) *Всяка група от ред n е изоморфна на някоя подгрупа на симетричната група S_n от n-степен.*

Дефиниция 1.1.6 *Една група G се нарича* ***циклична****, ако съществува елемент $g \in G$, такъв че за всяко $x \in G$ е изпълнено $x = g^k$ за някое $k \in Z$. Елементът g се нарича* ***пораждащ (образуващ) на*** *G.*

Пример 1.1.7 Адитивната група от целите числа $< \mathbb{Z}, + >= \{0, \pm 1, \pm 2, \ldots\}$ е пример за безкрайна циклична група. Ролята на пораждащ може да се изпълнява от два елемента: 1 и -1.
Множеството от всички n-ти корени на единицата в $\mathbb{C}$, т. е.

$$C_n = \{1, \epsilon, \epsilon^2, \ldots, \epsilon^{n-1}\}, \quad \epsilon = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n},$$

е циклична група с n елемента относно умножението на комплексни числа.
Пример на адитивна циклична група с ред n е съвкупността от възможните остатъците по модул n, т. е.

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\},$$

относно събирането по модул n. Лесно се вижда, че в тази група всяко число, което е взаимно просто с n изпълнява ролята на пораждащ елемент (т. е. $\mathbb{Z}_n$ има $\varphi(n)$ образуващи).

Дефиниция 1.1.7 *Нека G е група. **Ред** на елемента $g \in G$ наричаме минималното естествено число m, такова че $g^m = 1$ ($m.g = 0$ в адитивен запис). Ако такова естествено число не съществува казваме, че g има **безкраен ред**.*

В една крайна група, очевидно, всеки елемент има краен ред. В безкрайна циклична група всеки елемент е с безкраен ред (но това не е вярно за всяка безкрайна група).

Ето и някои свойства на цикличните групи:

Твърдение 1.1.8 *Всяка безкрайна група е изоморфна на $< \mathbb{Z}, + >$.*

Твърдение 1.1.9 *Всяка крайна група с ред n е изоморфна на C_n.*

Упражнение 1.1.1 *Покажете, че $\mathbb{Z}_n \cong C_n$.*

Горните две твърдения показват, че с точност до изоморфизъм има точно една циклична група от всеки ред.

Твърдение 1.1.10 *В безкрайна циклична група точно два елемента могат да бъдат пораждащ, а в циклична група с ред n - точно $\varphi(n)$.*

Теорема 1.1.11 *Всяка подгрупа на циклична група е циклична. Подгрупите на $< \mathbb{Z}, + >$ се изчерпват с множествата $k\mathbb{Z} = \{0, \pm k, \pm 2k, \pm 3k, \ldots\}$. Ако G е циклична група с ред n, то за всяко естествено число d делящо n съществува единствена подгрупа H на G с ред $|H| = d$ и с това се изчерпват всички подгрупи на G.*

Дефиниция 1.1.12 *Нека G е група и S нейно подмножество. Минималната (по включванекато множества) подгрупа H на G се нарича **подгрупа породена от** S и бележи с $H = \langle S \rangle$ или $H = \langle s_1, s_2, \ldots, s_t \rangle$, ако $S = \langle s_1, s_2, \ldots, s_t \rangle$. Ако $H \equiv G$ казваме, че S поражда G и че е множество от **пораждащи (образуващи) на** G. Всяко минималното по мощност множество от пораждащи се нарича **минимална система образуващи на** G.*
*Ако S е крайно множество казваме, че групата е **крайно породена**, в противния случай говорим за **безкрайно породена** група.*

Твърдение 1.1.13 *$\langle S \rangle$ съвпада със сечението на всички подгрупи на G, които съдържат S и*

$$\langle S \rangle = \{x_1 x_2 \ldots x_n \mid x_j = s_i \text{ or } x_j = s_i^{-1}\},$$

е съвкупността от възможните произведения на елементи от S или техните обратни.

Дори от крайно множество S може да получим безброй много от горните произведения, но много от тях могат да съвпадат, т. е. да задават един и същи елемент на групата (със сигурност това е така, ако G е крайна група). Съвкупността от всички равенства между тези произведения се нарича система от определящи отношения (тъждества). В тази съвкупност някои тъждества могат да се извлекат от други, т. е. може само с част от тъждествата да се получат всички образуващи отношения. Минимални по мощност

такива подсистеми се наричат **минимална система определящи отношения**. Например, ако G е циклична група с пораждащ g от ред n, то има само n произведения: $1, g, g^2, \ldots, g^{n-1}$. Минималната система определящи отношения в случая се състои само от $g^n = 1$.
Елементарната абелева 2-група с 4 елемента $A = \{1, a, b, ab\}$ има за минимална система определащи отношения три равенства: $a^2 = 1,\ b^2 = 1,\ ab = ba$. с тяхна помощ всяко произведение от елементите a, b или техните обратни може да се сведе към горните 4 елемента. Затова представянето на A в термините на образуващи и определящи отношения изглежда така:

$$A = \{a, b \mid a^2 = b^2 = 1,\ ab = ba\}.$$

Пример 1.1.8 Да разгледаме група D_n зададена абстрактно в термините на определящи отношения и образуващи с

$$D_n = \{a, b \mid a^n = b^2 = 1\ ab = ba^{n-1}\}.$$

Лесно се проверява, че тя се състои от $2n$ елемента, а именно

$$D_n = \{1, a, a^2, \ldots, a^{n-1}, b, ba, \ldots, ba^{n-1}\}.$$

Тази група се нарича **диедрална група** (произходът на името ще стане ясен в трета глава).

Дефиниция 1.1.14 *Нека е G група, а H нейна собствена подгрупа.* ***Ляв (десен) съседен клас на G по подгрупата H с представител g*** *наричаме множеството*

$$gH \stackrel{\text{def}}{=} \{gh \mid h \in H\}, \quad (\textit{съответно} \quad Hg \stackrel{\text{def}}{=} \{hg \mid h \in H\}).$$

Твърдение 1.1.15 *Следните две твърдения са еквивалентни:*

1. $aH = bH$ *(съответно* $Ha{=}Hb$*);*
2. $a^{-1}b \in H$ *(съответно* $ba^{-1} \in H$*).*

Два леви (десни) съседни класове, или съвпадат, или не се пресичат. Разбиването на G на съседни класове по H задава релация на еквивалентност в G.

Твърдение 1.1.16 *Всеки съседен клас на на G по подгрупата H е равномощен с H. Съществува взаимно-еднозначно съответствие между съвкупността от левите съседни класове по H и тази от десните съседни класове.*

Горното твърдение ни позволява да дадем следната дефиниция:

Дефиниция 1.1.17 ***Индекс на подгрупата H в G,*** *бележим $(G : H)$, наричаме мощността на множеството от левите (десните) съседни класове на G по H.*

Теорема 1.1.18 (Теорема на Лагранж) *Ако G е крайна група, а H нейна подгрупа, то*

$$|G| = |H|(G : H).$$

Следствие 1.1.19 *Редът и индексът на всяка подгрупа на една крайна група е делител на реда на групата.*

Следствие 1.1.20 *Редът на всеки елемент на една крайна група е делител на реда на групата.*

Теорема 1.1.21 *Групата $G \neq \{1\}$ няма собствени подгрупи тогава и само тогава, когато $G \cong C_p\,(\cong \mathbb{Z}_p)$ за някое просто число p.*

Теоремата на Лагранж и следствията от нея ни дават възможните редове на елементите и подгрупите в една група, но не гарантират за даден делител d съществуването на елемент или подгрупа с такъв ред. Например $|S_4| = 24$, но не съществуват, нито елемент, нито подгрупа с ред 6 (виж следващата глава).

1.2 Нормални подгрупи. Конструиране на групи

В този параграф ще опишем как от дадени групи можем да конструираме нови групи.

Дефиниция 1.2.1 *Нека G е група. Подгрупата $N \subseteq G$ наричаме* ***нормална (инвариантна) подгрупа****, ако $gN = Ng$ за всяко $g \in G$, т. е. разлаганията на леви и десни съседни класове съвпадат. Бележим $N \lhd G$.*

Теорема 1.2.2 *Следните твърдения са еквивалентни:*

1. $N \lhd G$;
2. $gNg^{-1} \equiv N, \quad$ *за всяко* $\quad g \in G$;
3. $gNg^{-1} \subseteq N, \quad$ *за всяко* $\quad g \in G$.

Пример 1.2.1 Всяка подгрупа с индекс 2 е нормална. Наистина $G = H \cup gH = H \cup Hg$, което влече $gH = Hg$.
В абелева група всички подгрупи са нормални.

Дефиниция 1.2.3 *Казваме, че $y \in G$ е* ***спрегнат с*** *$x \in G$, ако съществува $g \in G$, такова че $y = gxg^{-1}$. Изображението $\varphi_g : G \to G$, зададено с правилото $\varphi_g(x) = gxg^{-1}$ се нарича* ***вътрешен автоморфизъм*** *на G.*

Лесно се проверява, че $\varphi_g \in \mathrm{Aut}(G)$ и спрягането е релация на еквивалентност. Вътрешните автоморфизми образуват подгрупа на $\mathrm{Aut}(G)$, която бележим с $\mathrm{Inn}(G)$. Теорема 1.2.2 показва, че една подгрупа N е нормална тогава и само тогава, когато е инвариантна относно $\mathrm{Inn}(G)$, т. е. $\varphi_g(N) \subseteq N$ за всяко $g \in G$.

Дефиниция 1.2.4 ***Ядро*** *на хомоморфизма $\varphi : G \to G'$ (бележим с $\ker\varphi$) наричаме съвкупността от всички елементи на G, които се изобразяват от φ в единичния елемент на G', т. е.*

$$\ker\varphi \stackrel{\text{def}}{=} \{x \in G \mid \varphi(x) = 1_{G'}\}.$$

Следното твърдение показва също връзката между хомоморфизми и нормални подгрупи:

Твърдение 1.2.5 *Ядрото на всеки хомоморфизъм G в G' е нормална подгрупа на G.*

Всъщност твърдението задава обширен клас от примери на нормални групи и в този смисъл обосновава въвеждането на понятието нормална подгрупа.

Нека $N \triangleleft G$. В множеството

$$G/N \stackrel{\text{def}}{=} \{gN \mid g \in G\}$$

дефинираме умножение по правилото

$$g_1N.g_2N \stackrel{\text{def}}{=} (g_1g_2)N \quad \text{(в адитивен запис:} \quad (g_1+N)+(g_2+N) \stackrel{\text{def}}{=} (g_1+g_2)+N \text{)}$$

Твърдение 1.2.6 *Ако $N \triangleleft G$, то G/N е групата с единица (нула) N относно така въведената бинарна операция.*

Горното твърдение е вярно само ако N е нормална подгрупа!

Дефиниция 1.2.7 ***G/N*** *се нарича* ***фактор група на*** *G* ***по подгрупата*** *N.*

Изображението $\nu : G \to G/N$ дефинирано чрез $\nu(g) = gN$ е епиморфизъм и се нарича **естествен епиморфизъм на G върху G/N** (очевидно е епиморфизъм).

Теорема 1.2.8 (Основна теорема за хомоморфизмите) *Нека φ е хомоморфизъм на групата G в групата G'. Тогава $G/\ker\varphi \cong \mathrm{Im}(\varphi) \subseteq G'$, по-точно съществува единствен изоморфизъм η; $G/\ker\varphi \to \mathrm{Im}(\varphi)$, такъв че*

$$\varphi = \eta\nu.$$

Теорема 1.2.9 (Първа теорема за изоморфизмите) *Нека H е подгрупа и нека K е нормална подгрупа на G. Тогава $H \cap K$ е нормална подгрупа на H и $H/(H \cap K) \cong HK/K$.*

Теорема 1.2.10 (Втора теорема за изоморфизмите) *Нека $K \subseteq H \subseteq G$, където H и K са нормални подгрупи на G. Тогава $(G/K)/(H/K) \cong G/H$.*

Някои автори наричат горните три теореми съответно първа, втора и трета теорема за изоморфизмите.

Директно произведение и директна сума.

Нека G и H са две (мултипликативно записани) групи и да разгледаме тяхното декартово произведение, т. е. множеството $G \times H = \{(g,h) \mid g \in G, h \in H\}$ от наредени двойки на елементи от G и H. Дефинираме бинарна операция в $G \times H$ с правилото

$$(g_1,h_1)(g_2,h_2) = (g_1g_2, h_1h_2),$$

$g_1, g_2 \in G$ и $h_1, h_2 \in H$. Лесно се провериява, че $G \times H$ е група относно тази операция.

Дефиниция 1.2.11 *Групата $G \times H$ с покомпонентната бинарна операция (описана по-горе) се нарича* ***директно произведение*** *на групите G и H. Ако те са адитивно записани бинарната операция се дефинира като покомпонентно събиране и се нарича* ***директна сума****. Бележи се с $G \oplus H$.*

Индуктивно може да се дефинира директно произведение (сума) на повече от две групи, тъй като както лесно се вижда действието "вземане директно произведение" е асоциативно. Например, директното произведение на $n > 1$ копия на цикличната група C_p от ред p, $C_p^n = \underbrace{C_p \times C_p \times \cdots \times C_p}_{n}$ е абелева група от ред p^n и се нарича ***елементарна абелева p-група***.

Теорема 1.2.12 *Групата G е директно произведение на своите подгрупи A и B, т. е. $G \cong A \times B$, тогава и само тогава, когато*

$$G = AB,\ A \cap B = \{1\}\ и\ A, B \lhd G.$$

Теорема 1.2.13 *Нека $G \cong A \times B,\ A_1 \lhd A,\ B_1 \lhd B$. Тогава $(A_1 \times B_1) \lhd G$ и*

$$G/(A_1 \times B_1) \cong (A/A_1) \times (B/B_1).$$

Пример 1.2.2 Нека p, q са прости числа. Всяка абелева група G от ред pq е директно произведение на подгрупи от ред p и q, т. е. $G \cong C_p \times C_q$. Наистина всеки елемент на G има ред p, q, или pq. Ако съществува елемент $g \in G$ с ред $o(g) = pq$, то $G =< g >$ е циклична и следователно $a = g^q$ и $b = g^p$ имат редове p и q, съответно. Но тогава $< a >$ и $< b >$ са нормални подгрупи (G е абелева) и $G =< a > \times < b >$. Да предположим, че елементите на групата имат ред само p (или само q). Нека a е един такъв елемент. Тогава редът на фактор-групата $|G/ < a > | = q$ и следователно съществува $b \in G$, такъв че $(b < a >)^q =< a >$, т. е. $b^q \in < a >$. Но тогава $b^q = 1$ или $b^{qp} = 1$, т. е. достигаме противоречие (попадаме в предния случай).

Библиография

[1] А.И. Кострикин, *Въведение в алгебрата* (превод от руски), Наука и изкуство, София, 1981.

[2] Пл. Сидеров, *Записки по алгебра (групи, пръстени, полиноми),* ВЕДИ, София.