ЛЕКЦИЯ 8

ПРИМЕРЫ ДЕЙСТВИЙ

НОРМАЛИЗАТОРЫ ПОДГРУПП

КЛАССЫ СОПРЯЖЕННЫХ ЭЛЕМЕНТОВ

ЦЕНТР p-ГРУППЫ

ГРУППЫ ПОДСТАНОВОК

ПРОСТЫЕ ГРУППЫ

ПРИМЕРЫ ПОЛИГОНОВ

Пример 1. $M_G = \{1, 2, \ldots, n\}_{S_n}$, где σi — значение подстановки $\sigma \in S_n$ на элементе i из $\{1, 2, \ldots, n\}$. Так как $i(i, j) = j$ для цикла (i, j), то это действие группы $\mathbf{S}_n$ на $\{1, 2, \ldots, n\}$ транзитивно. Ясно, что, например, $\mathrm{St}\,(n) = \mathbf{S}_{n-1}$. Более общим образом, для любого множества M и группы всех биекций $\mathbf{S}(M)$ имеем полигон $M_{\mathbf{S}(M)}$.

Пример 2. Пусть $\sigma \in \mathbf{S}_n$, (σ) — циклическая подгруппа в $\mathbf{S}_n$, порожденная подстановкой σ. Тогда: $\{1, 2, \ldots, n\}_{(\sigma)}$ — полигон над группой (σ), его различные орбиты — это в точности непересекающиеся циклы подстановки (σ), перестановочные между собой.

Пример 3 (регулярное представление левыми умножениями). Пусть $M_G = G_G$ с умножением $(g, x) \to gx$ для $x \in G$, $g \in G$. Ясно, что: $(hg)x = h(gx)$ (для $x, g, h \in G$, ассоциативность умножения в группе); $ex = x$ для единицы e группы G.

Если $p, x \in G$, то $\mathrm{St}\,(p) = \{g \in G \mid gp = p\} = \{e\}$ и $\mathrm{Orb}\,(x) = Gx = G$ (т. е. это действие транзитивно).

Если $g \in G$, то рассмотрим отображение $\rho_g \colon G \to G$, $\rho_g x = gx$. Так как из $gx = gy$ для $x, y \in G$ следует (умножим на g^{-1} справа в группе G), что $x = y$, то ρ_g — мономорфизм. Так как для любого $z \in G$ имеем $z = gg^{-1}z$, то ρ_g — сюръекция. Итак, $\rho_g \in \mathbf{S}(G)$.

Так как для $x, g, h \in G$ имеем

$$\rho_{hg} x = (hg)x = h(gx) = \rho_h(\rho_g x),$$

т. е. $\rho_{hg} = \rho_h \rho_g$, то отображение $\rho \colon G \to \mathbf{S}^{\mathrm{r}}(G)$, $\rho(g) = \rho_g$, является гомоморфизмом групп.

Если $g, g' \in G$ и $\rho_g = \rho(g) = \rho(g') = \rho_{g'}$, то $g = eg = eg' = g'$. Таким образом, ρ — инъективный гомоморфизмом.

Итак, мы доказали следующее утверждение.

Теорема 1 (Кэли). *Регулярное представление группы G правыми умножениями*

$$G \xrightarrow{\rho} \mathbf{S}^{\mathrm{r}}(G) = \mathbf{S}(G), \quad g \to \rho_g, \quad \rho_g x = gx,$$

является инъективным гомоморфизмом.

Следствие 1. *Всякая группа G изоморфна некоторой подгруппе G' группы подстановок $\mathbf{S}(G)$ на множестве G.*

Следствие 2. *Если $n = |G| < \infty$, то группа G изоморфна некоторой подгруппе G' группы подстановок $\mathbf{S}_n$. С точностью до изоморфизма существует лишь конечное число групп порядка n.*

Замечание 1. К сожалению, $|S_n| = n!$, и подгрупп в $\mathbf{S}_n$ из n элементов достаточно много.

Пример 4. Пусть H — подгруппа группы G, рассмотрим полигон $M_H = G_H$, $(hx) \to hx$ для $x \in G$, $h \in H$. Если $p, x \in G$, то $\mathrm{St}\,(p) = \{h \in H \mid hp = p\} = \{e\}$ и $\mathrm{Orb}\,(x) = Hx$ — левы й смежный класс Hx по подгруппе H, порожденный элементом $x \in G$. Таким образом, в этом частном случае полигона G_H разбиение на орбиты превращается в хорошо знакомое нам разбиение группы в объединение непересекающихся различных левых смежных классов $G = \dot{\bigcup} Hx$, и как следствие подсчета элементов по орбитам имеем

$$|G| = \sum |\,\mathrm{Orb}\,(x)| = \sum |Hx| = [G : H]|H|$$

(т. е. теорему Лагранжа).

Пример 5 (действие группы $\boldsymbol{G}$ левыми умножениями на множестве правых смежных классов). Пусть H — подгруппа группы G,

$$M_G = \{xH,\ x \in G\}, \quad g(xH)g = gxH \ \text{ для } \ x, g \in G$$

(это умножение корректно: если $xH = x'H$, то $x' = xh$, $h \in H$, и поэтому $gx' = gxh$, тогда $gx'H = gxH$). Если $x, g_1, g_2 \in G$, то $(g_1g_2)(xH) = g_1\big(g_2(xH)\big)$ и $e(xH) = xH$, т. е. $M_G = \{xH \mid x \in G\}_G$ — правый полигон над группой G. Так как $\mathrm{Orb}\,(xH) = M_G$, то это действие группы G транзитивно.

Пример 6 (действие группы $\boldsymbol{G}$ на группе $\boldsymbol{G}$ сопряжением). Пусть $M_G = G_G$, $(g, m) \to gmg^{-1} = \alpha_g m$ для $m, g \in G$. Так как для $m, g, h \in G$ имеем

$$m\alpha_{hg} = (hg)m(hg)^{-1} = h(gmg^{-1})h^{-1} = \alpha_h(\alpha_g m),$$

т. е. $\alpha_{hg} = \alpha_h\alpha_g$,

$$\alpha_e m = eme^{-1} = m,$$

то $M_G = G_G$ с сопряжением — левый G-полигон.

НОРМАЛИЗАТОРЫ ПОДГРУПП

Пример 7. Пусть $L_G = L(G)$ — совокупность всех подгрупп H группы G, $(g, H) \to gHg^{-1}$, $g \to G$ (действие группы G на подгруппах сопряжением).

Определение 1. Стабилизатор подгруппы H при этом действии группы G сопряжениями $\mathrm{St}\,(H) = \{g \in G \mid gHg^{-1} = H\}$ называется *нормализатором подгруппы* H в группе G (для него используется обозначение $\mathbf{N}_G(H)$).

Итак, $\mathbf{N}_G(H) = \mathrm{St}\,(H) = \{g \in G \mid gHg^{-1} = H\}$.

Лемма 1 (свойства нормализатора $\mathbf{N_G(H)}$).

1) $\mathbf{N}_G(H)$ — *подгруппа группы* G, *содержащая подгруппу* H;

2) $H \lhd \mathbf{N}_G(H)$;

3) *если* $H \lhd K \subseteq G$ (*т. е.* K — *подгруппа группы* G, *содержащая подгруппу* H *и* H — *нормальная подгруппа в* K), *то* $K \subseteq \mathbf{N}_G(H)$, *и, таким образом,* $\mathbf{N}_G(H)$ — *наибольшая подгруппа, содержащая* H *в качестве нормальной подгруппы* (*конечно, если* $H \lhd G$, *то* $\mathbf{N}_G(H) = G$).

Доказательство.

1) Так как $\mathbf{N}_G(H) = \mathrm{St}\,(H)$, то ясно, что $\mathbf{N}_G(H)$ (как любой стабилизатор) — подгруппа группы G.

2) Если $g \to \mathbf{N}_G(H)$, то $gHg^{-1} = H$, т. е. $H \lhd \mathbf{N}_G(H)$ (т. е. H — нормальная подгруппа группы $\mathbf{N}_G(H)$).

3) Если $H \lhd K \subseteq G$, то для любого элемента $g \in K$ имеем $gHg^{-1} = H$ (поскольку H — нормальная подгруппа группы), т. е. $g \in \mathrm{St}\,(H) = \mathbf{N}_G(H)$, и поэтому $K \subseteq \mathbf{N}_G(H)$. □

Упражнение 1. Если B — подгруппа, лежащая в нормализаторе $\mathbf{N}_G(A)$ подгруппы A группы G, то AB — подгруппа группы G и $AB/A \cong B/A \cap B$.

КЛАССЫ СОПРЯЖЕННЫХ ЭЛЕМЕНТОВ

Если $x \in G$, то при сопряжении орбита элемента

$$\mathrm{Orb}\,(x) = \{gxg^{-1} \mid g \in G\} —$$

это класс сопряженных элементов элемента x.

Ясно, что $\operatorname{Orb}(e) = \{e\}$. Более того, $|\operatorname{Orb}(x)| = 1 \iff x \in \mathbf{Z}(G)$, т. е. одноэлементные орбиты — это в точности элементы центра, поскольку $gxg^{-1} = x$ для всех $g \in G$ равносильно тому, что $xg = gx$ для всех $g \in G$, т. е. тому, что $x \in \mathbf{Z}(G)$.

Ясно, что

$$\operatorname{St}(x) = \{g \mid gxg^{-1} = x\} = \mathbf{C}(x),$$

где $\mathbf{C}(x) = \{y \in G \mid xg = gx\}$ — централизатор элемента $x \in G$.

Таким образом, теорема о разбиении на орбиты в данном случае означает следующее.

Теорема 2 (о разбиении на классы сопряженных элементов). *Пусть G — группа, тогда*:

1) *группа является объединением орбит — непересекающихся различных классов сопряженных элементов (т. е. отношение сопряженности $y \sim x$, если $y = gxg^{-1}$, является отношением эквивалентности)*;

2) *число элементов конечной группы G, сопряженных с элементом $x \in G$, равно индексу централизатора $\mathbf{C}(x)$ элемента $x \in G$ в группе (поскольку $|G| = |\operatorname{Orb}(x)| \cdot |\operatorname{St}(x)| = \{$число сопряженных с x элементов$\} \cdot |\mathbf{C}(x)|$), т. е. числу $|G|/|\mathbf{C}(x)|$, и является делителем числа $|G|$.* □

Упражнение 2. Разбиение на классы сопряжённых элементов в группе подстановок $\mathbf{S}_n$ определяется типом циклового разложения (т. е. две подстановки в $\mathbf{S}_n$ сопряжены тогда и только тогда, когда они имеют одинаковые цикловые разложения, т. е. для каждого числа r одинаковое число циклов длины r в их цикловых разложениях).

ЦЕНТР КОНЕЧНОЙ p-ГРУППЫ

Теорема 3. *Фактор неабелевой группы по ее центру не может быть циклической группой.*

Доказательство. Предположим, что это не так, т.е. существует некоторая неабелева группа G такая, что $G/\mathbf{Z}(G) = G/Z$ — циклическая группа. Пусть тогда $G/Z = \langle gZ \rangle$. В этом случае любой элемент группы G представляется в виде произведения $g^k z$, где $z \in Z$.

Рассмотрим два произвольных элемента группы G — $g^k z_1$ и $g^l z_2$. Они коммутируют, так как элементы центра коммутируют со всеми элементами группы, а степени элемента g коммутируют между собой.

Таким образом, группа G — абелева, что противоречит предположению. □

Теорема 4. *Пусть G — конечная p-группа, т. е. $|G| = p^k$, где p — простое число, $k \in \mathbb{N}$. Тогда ее центр нетривиален, т. е. $|\mathbf{Z}(G)| > 1$.*

Доказательство. Рассмотрим разбиение группы G на классы сопряженных элементов. Одноэлементный класс — это в точности элемент центра (один из них $\{e\}$). Содержащий больше одного элемента класс сопряженных элементов содержит p^l элементов, где $l > 1$ (как нетривиальный делитель числа $|G| = p^k$). Отсюда следует, что $|\mathbf{Z}(G)| > 1$ (в противном случае $p^k = 1 + pq$). □

Теорема 5 (о коммутативности группы из $\boldsymbol{p^2}$ элементов). *Пусть G — конечная группа, $|G| = p^2$, где p — простое число. Тогда G — абелева (т. е. коммутативная) группа.*

Доказательство. В силу предыдущей теоремы $|\mathbf{Z}(G)| > 1$, т. е. $|\mathbf{Z}(G)| = p$ или $|\mathbf{Z}(G)| = p^2$. Но первый случай ($|\mathbf{Z}(G)| = p$) невозможен, поскольку тогда $|G/\mathbf{Z}(G)| = p^2/p = p$, и поэтому $G/\mathbf{Z}(G)$ — циклическая группа, что невозможно. Итак, $|\mathbf{Z}(G)| = p^2$, т. е. $G = \mathbf{Z}(G)$, и поэтому группа G коммутативна. □

Теорема 6. *Пусть G — p-группа, $|G| = p^r$, $r \geq 1$. Тогда группа G содержит нормальную подгруппу порядка p^{r-1}.*

Доказательство. Проведем индукцию по r. Ясно, что утверждение верно при $r = 1$. Пусть оно верно для всех $k < r$, где $r > 1$.

В силу теоремы 4 $Z(G) \neq e$ (здесь $Z(G)$ — центр группы G). Так как p делит число $|Z(G)|$, то абелева группа $Z(G)$ содержит элемент g такой, что $p = O(g) = |\langle g \rangle|$. Ясно, что $N = \langle g \rangle \lhd G$ и $|G/N| = p^r/p = p^{r-1}$. В силу индуктивного предположения для p^{r-2} фактор-группа $\bar{G} = G/N$ содержит нормальную подгруппу $\bar{H} = H/N$, где H — нормальная подгруппа в G, $N \subset H \lhd G$, $|\bar{H}| = p^{r-2}$. Тогда $|H| = |\bar{H}|\,|N| = p^{r-2} \cdot p = p^{r-1}$. Итак, группа G содержит нормальную подгруппу H порядка p^{r-1}. □

ГРУППЫ ПОДСТАНОВОК

Напомним, что мы рассматриваем группу подстановок $\mathbf{S}_n$ с записью умножения слева от аргумента: $(\sigma\tau)(i) = \sigma\big(\tau(i)\big)$.

Заметим, что:

$$(i_1\, i_2\, \ldots\, i_k) = (i_1\, i_k)(i_1\, i_{k-1}) \ldots (i_1\, i_2)$$

(в частности, $(1\,2\,\ldots\,k) = (1\,k)(1\,k-1)\ldots(1\,2)$); $(i\,j) = (1\,i)(1\,j)(1\,i)$ для $1 \neq i$, $1 \neq j$.

Нам будут полезны разные системы образующих группы $\mathbf{S}_n$:

$$\mathbf{S}_n = \langle (i\,j),\ i \neq j \rangle = \langle (1\,2), (1\,3), \ldots, (1\,n) \rangle.$$

Лемма 2.

$$\tau(1, 2, \ldots, k)\tau^{-1} = \big(\tau(1), \ldots, \tau(k)\big)$$

$(\tau^{-1}(1, 2, \ldots, k)\tau = (\tau^{-1}(1), \ldots, \tau^{-1}(k))$.

Доказательство. Если $\sigma(i) = j$, $\tau(i) = s$, $\tau(j) = t$, то

$$(\tau\sigma\tau^{-1})(s) = (\tau\sigma\tau^{-1})\big(\tau(i)\big) = (\tau\sigma)(i) = \tau(j) = t. \qquad \square$$

Теорема 7. *Две подстановки $\sigma, \gamma \in \mathbf{S}_n$ сопряжены тогда и только тогда, когда они имеют одинаковое цикловое разложение.*

Доказательство.

1) Если $\gamma = \tau\sigma\tau^{-1}$ и $\sigma = \sigma_1 \ldots \sigma_r$ — разложение подстановки σ в произведение циклов с непересекающимися орбитами, то

$$\gamma = (\tau\sigma_1\tau^{-1})(\tau\sigma_2\tau^{-1}) \ldots (\tau\sigma_r\tau^{-1}),$$

$\{\tau\sigma_i\tau^{-1}\}$ — циклы, орбиты которых являются образами орбит циклов σ_i, и поэтому эти орбиты дают разбиение множества $\{1, 2, \ldots, n\}$. Таким образом, подстановки γ и σ имеют одинаковые цикловые разложения.

2) Если γ и σ имеют одинаковое цикловое разложение, то соответствие между элементами соответствующих орбит приводит нас к биекции τ, т. е. $\sigma \in \mathbf{S}_n$, для которой $\gamma = \tau\sigma\tau^{-1}$. $\square$

Лемма 3. *Для циклов длины* 2 τ_1, τ_2 (*т. е. для транспозиций*) *группы* $\mathbf{S}_n$ *при* $n \geq 3$ *произведение* $\tau_1\tau_2$ *либо* 3*-цикл, либо произведение двух* 3*-циклов.*

Доказательство.

Случай 1. Если $\tau_1 = \tau_2$, то

$$\tau_1\tau_2 = \tau_1^2 = e = (i\,j\,k)(k\,j\,i).$$

Случай 2. $\tau_1 \neq \tau_2$.

2а) орбиты пересекаются (по одному элементу i):

$$(i\,k)(i\,l) = (i\,l\,k),$$

здесь $k \neq l$.

2б) Орбиты транспозиций τ_1 и τ_2 не пересекаются:

$$(i\,j)(k\,l) = (i\,l\,j)(i\,l\,k). \qquad \square$$

Теорема 8. $\mathbf{A}_n = \langle\{(i\,j\,k)\}\rangle = \langle(1\,2\,3), (1\,2\,4), \ldots, (1\,2\,n)\rangle$ *при* $n \geq 3$.

Доказательство.

1) Если $\sigma \in \mathbf{A}_n$, $n \geq 3$, то $\sigma = \tau_1 \ldots \tau_{2m}$, где τ_i — транспозиция (цикл длины 2). Так как $\tau_{2i-1}\tau_{2i}$ — или 3-цикл, или произведение двух 3-циклов, то

$$\mathbf{A}_n = \langle\{(i,j,k)\}\rangle.$$

2)

$$\begin{aligned}
(i\,j\,k) &= (1\,2\,i)(2\,j\,k)(1\,2\,i)^{-1};\\
(2\,j\,k) &= (1\,2\,j)(1\,2\,k)(1\,2\,j)^{-1};\\
(1\,j\,k) &= (1\,2\,k)^{-1}(1\,2\,j)(1\,2\,k).
\end{aligned} \qquad \square$$

Упражнение 3. $\mathbf{A}_5 = \langle (2\,5\,4), (1\,2\,3\,4\,5) \rangle$.

Теорема 9.

1) $[\mathbf{S}_2, \mathbf{S}_2] = \{e\}$; $[\mathbf{S}_n, \mathbf{S}_n] = \mathbf{A}_n$ *при* $n \geq 3$.

2) $[\mathbf{A}_3, \mathbf{A}_3] = \{e\}$;
$[\mathbf{A}_4, \mathbf{A}_4] = \mathbf{V}_4 = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$;
$[\mathbf{A}_n, \mathbf{A}_n] = \mathbf{A}_n$ *при* $n \geq 5$.

Доказательство.

1) Так как $[a, b] = a^{-1}b^{-1}ab$ для $a, b \in \mathbf{S}_n$ всегда является четной подстановкой, то $[\mathbf{S}_n, \mathbf{S}_n] \subseteq \mathbf{A}_n$.

Так как $\mathbf{A}_n = \langle \{(i\,j\,k)\} \rangle$ и

$$(i\,j\,k) = (i\,j)(i\,k)(i\,j)(i\,k) = [(i\,j), (i\,k)],$$

то $\mathbf{A}_n \subseteq [\mathbf{S}_n, \mathbf{S}_n]$.

2а) Ясно, что $[\mathbf{A}_3, \mathbf{A}_3] = \{e\}$ ($\mathbf{A}_3$ — абелева группа, $|\mathbf{A}_3| = 3$).

2б) Так как

$$[(i\,j\,k), (i\,j\,l)] = (k\,j\,i)(l\,j\,i)(i\,j\,k)(i\,j\,l) = (i\,j)(k\,l),$$
$$[(i\,j\,k), (i\,l\,j)] = (k\,j\,i)(j\,l\,i)(i\,j\,k)(i\,l\,j) = (i\,k)(j\,l),$$

то $\mathbf{V}_4 \subseteq [\mathbf{A}_4, \mathbf{A}_4]$.

Так как $|\mathbf{A}_4/\mathbf{V}_4| = 12/4 = 3$, то $\mathbf{A}_4/\mathbf{V}_4$ — абелева группа, поэтому $[\mathbf{A}_4, \mathbf{A}_4] \subseteq \mathbf{V}_4$. Итак, $[\mathbf{A}_4, \mathbf{A}_4] = \mathbf{V}_4$.

2в) При $n \geq 5$ для $\{i, j, k\}$ найдутся $l, m \notin \{i, j, k\}$, $l \neq m$. Поэтому

$$(i\,j\,k) = (i\,j\,m)(i\,k\,l)(m\,j\,i)(l\,k\,i) = [(m\,j\,i), (l\,k\,i)],$$

таким образом, $\mathbf{A}_n \subseteq [\mathbf{A}_n, \mathbf{A}_n]$, и следовательно, $\mathbf{A}_n = [\mathbf{A}_n, \mathbf{A}_n]$ при $n \geq 5$. □

Упражнение 4. Каждый элемент группы $\mathbf{A}_5$ является коммутатором.

ПРОСТЫЕ ГРУППЫ

Группа G называется *простой*, если у нее нет нормальных подгрупп $N \lhd G$, отличных от $\{e\}$ и G.

Замечание 2. Простые абелевы группы — это в точности циклические группы простого порядка. Действительно, в абелевой группе любая подгруппа нормальна. Поэтому простая абелева группа является циклической. В группе $\mathbb{Z}$ много подгрупп, в частности $2\mathbb{Z}$, т. е. она не является простой. Если $G = (a)$, $O(a) = n = kl$, то $(a^k) \subset (a)$, и группа G не является простой. Итак, $G(a)$ — простая группа тогда и только тогда, когда $|G| = \emptyset(a) = p$.

Замечание 3. Если $|G| = p^k$, $k > 1$, — конечная p-группа из p^k, $k > 1$, элементов, то G не является простой. Действительно, $e \neq \mathbf{Z}(G) \lhd G$.

Теорема о классификации конечных простых групп, видимо, завершена, ее полное связное доказательство создается.

Мы докажем теорему о том, что при $n \geq 5$ группа $\mathbf{A}_n$ является простой (в частности, $\mathbf{A}_5$ — простая группа).

Лемма 4. *При $n \geq 5$ любые два 3-цикла в группе $\mathbf{A}_n$ сопряжены.*

Доказательство. Пусть $\sigma_1 = (1\,2\,3)$, $\sigma_2 = (a\,b\,c) \in \mathbf{A}_n$, $n \geq 5$. Найдется $\tau \in \mathbf{S}_n$, для которой $\sigma_2 = \tau(1\,2\,3)\tau^{-1}$.

а) Если $\tau \in \mathbf{A}_n$, то все доказано.

б) Если $\tau \in \mathbf{S}_n \setminus \mathbf{A}_n$, то $\rho = \tau(4\,5) \in \mathbf{A}_n$, $(4\,5) \in \mathbf{C}_{\mathbf{A}_5}\big((1\,2\,3)\big)$. Тогда

$$\rho(1\,2\,3)\rho^{-1} = \tau(4\,5)(1\,2\,3)(4\,5)^{-1}\tau^{-1} = \tau(1\,2\,3)\tau^{-1} = \sigma_2. \qquad \square$$

Лемма 5. *Подстановки вида* $(1\,2)(3\,4)$ *и* $(a\,b)(c\,d)$ *сопряжены в* $\mathbf{A}_n$ *при* $n \geq 5$.

Доказательство. Пусть $m = 5$ (отличный от $1, 2, 3, 4$). Тогда $(3\,4\,m)(1\,2)(3\,4)(3\,4\,m)^{-1} = (1\,2)(4\,m)$. $\square$

Теорема 10. $\mathbf{A}_5$ — *простая* (*некоммутативная*) *группа.*

Доказательство. Пусть $\{e\} \neq H \lhd \mathbf{A}_5$.

Случай 1. Пусть $(a\,b\,c) \in H$. Тогда и все сопряженные с ним циклы длины 3 лежат в H, а циклы длины три порождают все $\mathbf{A}_5$, поэтому $H = \mathbf{A}_5$.

Случай. 2. $\alpha = (a\,b\,c\,d\,e) \in H$. Тогда

$$(a\,b)(c\,d)(a\,b\,c\,d\,e)(a\,b)(c\,d) = (b\,a\,d\,c\,e) \in H,$$
$$(b\,a\,d\,c\,e)(a\,b\,c\,d\,e) = (b\,e\,d) \in H,$$

и поэтому (случай 1) $H = \mathbf{A}_5$.

Случай 3. $(a\,b)(c\,d) \in H$. Тогда

$$(a\,b\,c\,e\,d) = (d\,e)(a\,c)(c\,d)(a\,b) \in H,$$

и (случай 2) поэтому $H = \mathbf{A}_5$. $\square$