Задача 0.1. *Можно ли разложить в прямое произведение собственных подгрупп следующие группы:* S_3, A_4, S_4, Q_8 *?*

Решение. В каждой из этих групп нет двух нетривиальных подгрупп, удовлетворяющих указанным выше свойствам, например, нет нетривиальных нормальных подгрупп, пересекающихся только по единице, и произведение порядков которых равно порядку группы, а, скажем, в Q_8 вообще нет нетривиальных подгрупп, пересекающихся только по единице. Поэтому нет, не разлагаются. $\square$

Задача 0.2. Найти $Q_8/\{\pm 1\}$.

Подгруппы в Q_8: $\{1, -1\}, \{1, -1, i, -i\}, \{1, -1, j, -j\}, \{1, -1, k, -k\}$.
Все подгруппы нормальны. Первая подгруппа – это C_2, остальные изоморфны C_4
$Q_8/\{1, -1\} = \{\{1, -1\}, \{i, -i\}, \{j, -j\}, \{k, -k\}\}$.
$Q_8/\{1, -1, i, -i\} = \{\{1, -1, i, -i\}, \{j, -j, k, -k\}$.
Первая факторгруппа изоморфна V_4, факторгруппы по трем подгруппам 4-го порядка изоморфны C_2.

Задача 0.3. Положим

$$G = \mathrm{GL}^+(n, \mathbb{R}) = \{A \in M_{n\times n} : \det A > 0\}, \;\; G_1 = \{\lambda E \mid \mathbb{R} \ni \lambda > 0\}, G_2 = \mathrm{SL}(n, \mathbb{R}).$$

Тогда $G \cong G_1 \times G_2$.

Доказательство. Подгруппы G_1, G_2 — нормальны и пересекаются только по единичной матрице. К тому же $G = G_1G_2 : \mathrm{GL}^+(n, \mathbb{R}) \ni A = \lambda A_1 = (\lambda E)A_1$, где $\lambda = \sqrt[n]{\det A}$, $A_1 = \frac{1}{\lambda}A \in \mathrm{SL}(n, \mathbb{R})$. Действительно, $\det\left(\frac{1}{\lambda}A\right) = \frac{1}{\lambda^n}\det A = \frac{\det A}{\det A} = 1$. $\square$

Задача 0.4. Верно ли, что при нечетном n группа $\mathrm{GL}(n, \mathbb{R})$ изоморфна $G_1 \times G_2$, где $G_1 = \{\lambda E \mid \mathbb{R} \ni \lambda \neq 0\}$, $G_2 = \mathrm{SL}(n, \mathbb{R})$?

Ответ: Да, верно.

[Поскольку корень отрицательной степени модно взять и у отрицательного числа, рассуждения из предыдущей задачи прямо переносятся на рассматриваемый случай.]

Задача 0.5. Докажите, что $S_n = A_n \leftthreetimes \langle(12)\rangle_2$.

Доказательство. Имеется равенство: $|S_n| = |A_n||\langle(12)\rangle_2|$. Также имеем
$A_n \lhd S_n$, $\langle(12)\rangle_2 < S_n$, и $A_n \cap \langle(12)\rangle_2 = \{e\}$. $\square$

Задача 0.6. Показать, что в предыдущей задаче вместо транспозиции (12) можно взять любую другую транспозицию.

Задача 0.7. Показать, что группу кватернионов Q_8 нельзя разложить ни в прямое, ни в полупрямое произведение своих подгрупп.

Решение. Группу кватернионов Q_8 нельзя разложить ни в прямое, ни в полупрямое произведение своих подгрупп, так как любая подгруппа Q_8 содержит 1 и -1, следовательно пересечение двух подгрупп (все подгруппы в Q_8 нормальны) содержит по крайней мере -1, не считая единицы. $\square$

Задача 0.8. $S_4 \cong V_4 \leftthreetimes S_3$. Как определяется $\varphi : S_3 \to \mathrm{Aut}\,(V_4)$?

Доказательство. Для начала вспомним, что $V_4 \lhd S_4$. Группа S_3 вложена в S_4 в виде подгруппы, оставляющей на месте 4. Для каждого $k \in \{1,2,3,4\}$ в V_4 имеется единственная подстановка, переводящая 4 в k. Значит, каждая подстановка $\sigma \in S_4$ предствляется единственным образом в виде $\sigma = \alpha\beta$, где $\alpha \in V_4, \beta \in S_3$.

Обозначим через $j : S_3 \to S_4$ описанное выше вложение группы S_3 в S_4 в качестве подгруппы. Тогда $\varphi_\tau(h) = i_{j(\tau)}(h)$ для $\tau \in S_3$, $h \in V_4$. □

Задача 0.9. *Показать, что*

$$GL(n,\mathbb{R}) = SL(n,\mathbb{R}) \leftthreetimes \left\{ \begin{pmatrix} \lambda & \dots & 0 \\ 0 & 1\dots & 0 \\ \dots & \dots & \dots \\ 0 & \dots & 1 \end{pmatrix} \in GL(n,\mathbb{R}) \mid \lambda \in \mathbb{R}^* \right\}.$$

Доказательство. Известно, что $\mathrm{SL}(n,\mathbb{R}) \lhd \mathrm{GL}(n,\mathbb{R})$.
Также ясно, что $SL(n,\mathbb{R}) \cap \left\{ \begin{pmatrix} \lambda & \dots & 0 \\ 0 & 1\dots & 0 \\ \dots & \dots & \dots \\ 0 & \dots & 1 \end{pmatrix} \mid \lambda \neq 0 \right\} = \{E\}$, где E — единичная матрица. Группа $\mathrm{GL}(n,\mathbb{R})$ представляется в виде произведения указанных подгрупп слеующим образом:

$$\mathrm{GL}(n,\mathbb{R}) \ni A = \widetilde{A} \cdot \begin{pmatrix} \det A & \dots & 0 \\ 0 & 1\dots & 0 \\ \dots & \dots & \dots \\ 0 & \dots & 1 \end{pmatrix},$$

где первый столбец матрицы $\widetilde{A}$ получается из первого столбца матрицы A делением всех элементов столбца на $\det A$, а остальные столбцы такие же как у A. Действительно, обозначим через C_λ диагональную матрицу из второй подгруппы. Тогда $C_{\lambda_1}C_{\lambda_2} = C_{\lambda_1\lambda_2}$, $C_1 = E$ и $\det C_\lambda = \lambda$. Имеем $A = AC_{\frac{1}{\lambda}}C_\lambda$. Возьмем $\lambda = \det A$ и положим $\widetilde{A} = AC_{\frac{1}{\lambda}}$. Тогда $\det \widetilde{A} = \det\left(AC_{\frac{1}{\lambda}}\right) = \det A \det C_{\frac{1}{\lambda}} = \det A / \det A = 1$ и $A = \widetilde{A}C_\lambda$. Это – требуемое разложение. Кроме того, умножение матрицы A справа на $C_{\frac{1}{\lambda}}$ изменяет только ее первый столбец – он делится на λ, т.е. на $\det A$. □

Задача 0.10. Можно ли в предыдущей задаче вместо второй подгруппы взять подгруппу матриц вида
$\{B_\lambda = (b_{ij}) \,|\, b_{nn} = \lambda \neq 0,\ b_{ii} = 1 \text{ для } 1 \leq i \leq n-1,\ b_{ij} = 0 \text{ при } i \neq j\}$?

Ответ: Да, можно.

Задача 0.11. Пусть $N = A_3$ и $H = C_2$. Найти все полупрямые произведения $N \leftthreetimes H$.

Решение. Группа четных подстановок $A_3 = \{e, (123), (132)\} = C_3 = \{e, a, a^2\}$ имеет порядок $|A_3| = 3$. Группа $C_2 = \{e, s\}$ – циклическая группа порядка 2.

Для того, чтобы найти все полупрямые произведения $C_3 \leftthreetimes C_2$, рассмотрим все возможные гомоморфизмы $\varphi : C_2 \longrightarrow \mathrm{Aut}\, \mathrm{C}_3$.

Случай 1: $\varphi(e_{C_2}) = \mathrm{id} = \mathrm{id}_{C_3}$, $\varphi(s) = \mathrm{id}$. Тогда $\mathrm{id}\,(e_{C_3}) = e$, $\mathrm{id}\,(a) = a$, $\mathrm{id}(a^2) = a^2$ и $C_3 \leftthreetimes_\varphi C_2 = C_3 \times C_2$ – прямое произведение.

Случай 2: $\varphi(e) = \mathrm{id}$, $\varphi(s) = \varphi_s : \varphi_s(e) = e, \varphi_s(a) = a^2$, $\varphi_s(a^2) = a$. Значит, $C_3 \leftthreetimes_\varphi C_2 = \{(e, e), (a, e), (a^2, e), (e, s), (a, s), (a^2, s)\}$.

Проверим получившуюся группу на коммутативность:

$$(a, e)(a^2, s) = (a\varphi_e(a^2), es) = (aa^2, s) = (e, s),$$
$$(a, s)(a^2, s) = (a\varphi_s(a^2), ss) = (a^2, e).$$

Групп 6-го порядка всего две: $C_6 \cong C_2 \times C_3$ и D_3. Но наша группа не коммутативна, следовательно, она изоморфна D_3. Итак,

$$A_3 \leftthreetimes \langle (12) \rangle_2 = S_3 \cong D_3.$$

Отметим, что во втором случае $\varphi_s(g) = g^{-1}$ для любого $g \in C_3$. $\square$

Задача 0.12. Пусть A – абелева группа.

1. Показать, что
$$D(A) = \{(a, \varepsilon) \mid a \in A, \varepsilon = \pm 1\}$$
с операцией умножения $(a_1, \varepsilon_1)(a_2, \varepsilon_2) = (a_1 a_2^{\varepsilon_1}, \varepsilon_1 \varepsilon_2)$ является группой.

2. Показать, что если $A =< a >_n$, то $D(A)$ изоморфна диэдральной группе D_n.

3. Показать, что $D(A) \cong A \leftthreetimes C_2$. Как определяется φ?

Верно ли, что $\varphi_1 = \mathrm{id}_A$, $\varphi_{-1}(a) = a^{-1}$?

Задача 0.13. Пусть группа A неабелева. Показать, что в этом случае умножение, введенное на $D(A)$ в предыдущей задаче, неассоциативно (тем самым $D(A)$ в этом случае даже не полугруппа).

Задача 0.14. Изоморфна ли группа $GL(n, \mathbb{R})$ прямому, или полупрямому, произведению групп $GL^+(n, \mathbb{R})$ и $C_2 = \{\pm 1\}$?

Указание: Если n нечетно, то подгруппа $\{\pm E\} \cong C_2$ нормальна и получается прямое произведение. Для произвольного n рассмотрим, например, подгруппу $\{E, \mathrm{diag}(-1, 1, \ldots, 1)\} \cong \mathrm{C}_2$. Получается полупрямое произведение.

Задача 0.15. Показать, что дробно линейные отображения расширенной комплексной плоскости образуют группу.

Доказательство. Расширенная комплексная плоскость: $\overline{\mathbb{C}} := \mathbb{C} \cup \{\infty\}$.

Дробно линейное отображение:

$$z \mapsto \frac{az + b}{cz + d}, \ \ a, b, c, d \in \mathbb{C}, \ \ ad - bc \neq 0.$$

$$-d/c \mapsto \infty, \ \ \infty \mapsto \lim_{z \to \infty} \frac{az + b}{cz + d} = a/c.$$

Дробно линейное отображение – биекция расширенной комплексной плоскости на себя. Композиция дробно линейных отображений является дробно линейным отображением.

Тождественное отображение $z \mapsto z$ является единицей этой группы. Обратное отображение к $z \mapsto \frac{az+b}{cz+d}$ – это дробно линейное отображение $z \mapsto \frac{dz-b}{-cz+a}$.

Сопоставляя матрице $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{C})$ дробно линейное отображение $z \mapsto \frac{az+b}{cz+d}$ получаем эпиморфизм. Ядро состоит из скалярных матриц. Фактор по ядру обозначается как $PGL(2, \mathbb{C})$ и называется проективной линейной группой.

Задача: Показать, что $PGL(2, \mathbb{C}) \cong PSL(2, \mathbb{C})$, где $PSL(2, \mathbb{C}) := SL(2, \mathbb{C})/\{\pm E\}$. □

Задача 0.16. Найти $Z(S_n)$ и $\operatorname{Int} S_n$ для $n \geqslant 3$.

Решение. Пусть $\alpha \in S_n$, и $\alpha \neq \mathrm{id}$, то есть существуют такие $i \neq j$, что $\alpha(i) = j$. Так как $n \geqslant 3$, то существует $k \leq n$, отличное от i и j. Рассмотрим $\beta = (jk)$. Тогда $\beta\alpha\beta^{-1}(i) = \beta\alpha(i) = \beta(j) = k$. Значит, $\beta\alpha\beta^{-1}(i) = k \neq j = \alpha(i)$, то есть подстановки α и β не коммутируют. Таким образом, мы показали, как для данной нам неединичной подстановки найти такую, которая с ней не коммутирует. Поэтому $Z(S_n) = \{e\}$.

$\operatorname{Int} S_n = S_n/Z(S_n) = S_n/\{e\} = S_n$. □

Задача 0.17. Доказать, что $Z(D_n) = \langle a^m \rangle$, если $n = 2m$, где a — поворот на угол $\frac{2\pi}{n}$, и $Z(D_n) = \{e\}$, если $n = 2m + 1$.

Задача 0.18. $Z(GL(n, \mathbb{C})) = \{\lambda E\}$, $\lambda \neq 0$

Задачи 0.19. 1. a) $\operatorname{End}(\mathbb{Z}) = \operatorname{Hom}(\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}$.

b) $\operatorname{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

2. a) $\operatorname{Hom}(\mathbb{Z}_m, \mathbb{Z}_n) = 0$, если $(m, n) = 1$.

b) $\operatorname{End}(\mathbb{Z}_m) = \operatorname{Hom}(\mathbb{Z}_m, \mathbb{Z}_m) = \mathbb{Z}_m$

3. $\operatorname{Hom}(A \oplus B, C) \cong \operatorname{Hom}(A, C) \oplus \operatorname{Hom}(B, C)$.

4. $\operatorname{Hom}(A, B \oplus C) \cong \operatorname{Hom}(A, B) \oplus \operatorname{Hom}(A, C)$.

5. Пусть $f\colon A \to F$ – эпиморфизм и F свободна.

Показать, что тогда $A = \ker f \oplus B$, где $B \cong F$.

6. Показать, что $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$ не являются конечно порожденными.

Задача 0.20. Сравнение $x^2 \equiv a \pmod{p}$ для a, не делящегося на простое $p > 2$, имеет два решения (отличающихся знаком), если $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, и не имеет решения, если $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Если решение есть, то a сравнимо с одним из чисел списка
$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$

[В силу малой теоремы Ферма $a^{p-1} = 1$ для a, не делящегося на простое $p > 2$, поэтому $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$.]

0.1 Силовские подгруппы

Определение 0.21. *Конечная группа G называется p-группой, где p – простое число, если ее порядок является степенью числа p, т. е. $|G| = p^n$.*

В частности, тривиальная группа (содержащая только единичный элемент) является p-группой для любого простого p. Поскольку по теореме Лагранжа порядок подгруппы делит порядок группы, мы видим, что любая подгруппа p-группы сама является p-группой.

Теорема 0.22. *Центр нетривиальной p-группы нетривиален.*

Предложение 0.23. *Всякая группа порядка p^2, где p - простое число, является абелевой.*

Абелевых групп порядка p^2 с точностью до изоморфизма всего две – циклическая $\mathbb{Z}_{p^2}$ и $\mathbb{Z}_p \oplus \mathbb{Z}_p$.

Определение 0.24. *Силовской p-подгруппой группы G называется всякая ее подгруппа, индекс которой не делится на p, т.е. любая подгруппа порядка p^n, где $|G| = p^n m$ и $(m, p) = 1$.*

Теорема 0.25. *Силовская p-подгруппа существует.*

Теорема 0.26. *Всякая p-подгруппа группы G содержится в некоторой силовской p-подгруппе. Все силовские p-подгруппы сопряжены.*

Теорема 0.27. *Число силовских p-подгрупп делит индекс силовской p-подгруппы и сравнимо с 1 по модулю p, т. е. если $|G| = mp^n$, где m не делится на p, то число силовских p-подгрупп делит m и сравнимо с 1 по модулю p.*

Пример 0.28. Положим $GL(n, q) := GL(n, \mathbb{F}_q)$, где $q = p^d$, p – простое число. Обозначим через $UT(n, q)$ подгруппу в $GL(n, q)$ верхне-треугольных матриц с 1-ми на главной диагонали. Покажем, что $UT(n, q)$ является силовской p-подгрупой в $GL(n, q)$.

Имеем $|GL(n, q)| = (q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1}) = \prod_{i=0}^{n-1}(q^n - q^i)$. Действительно, столбцы матрицы должны быть линейно независимы, поэтому первый столбец матрицы может быть любым ненулевым вектором из $\mathbb{F}_q^n$, т. е. имеем $q^n - 1$ возможностей, второй столбец – любым вектором не коллинеарным первому столбцу (дает $q^n - q$ вариантов), третий – любым вектором, не лежащим в двумерном подпространстве, натянутом на первые два столбца (дает $q^n - q^2$ вариантов), и т. д. Далее, имеем

$$|GL(n, q)| = \prod_{i=0}^{n-1}(q^n - q^i) = m \prod_{i=1}^{n-1} q^i = m\, q^{\sum_{i=1}^{n-1} i} = mq^{\frac{n(n-1)}{2}} = p^{\frac{dn(n-1)}{2}} m,$$

где $m = \prod_{i=0}^{n-1}(q^{n-i} - 1)$ и, следовательно, $(m, p) = 1$.

Число наддиагональных элементов в матрицах из $UT(n, q)$, которые могут быть произвольными элементами поля $\mathbb{F}_q$, равно $(n^2 - n)/2 = \frac{n(n-1)}{2}$. Поэтому $|UT(n, q)| = q^{\frac{n(n-1)}{2}} = p^{\frac{dn(n-1)}{2}}$, откуда и следует, что $UT(n, q)$ – силовская p-подгруппа группы $GL(n, q)$.

Задача 0.29. Если p – простой делитель порядка группы, то в группе существует элемент порядка p.

Решение. Возьмем какую-нибудь силовскую p-подгруппу. Из условия следует, что она нетривиальна, поэтому в ней имеется нетривиальный элемент a. Его порядок делит порядок силовской p-подгруппы и, следовательно, равен p^k с $k \geq 1$. Тогда $a^{p^{k-1}}$ – искомый элемент порядка p. $\square$

Задача 0.30. Показать, что всякая группа G порядка 45 абелева.

Решение. Обозначим через N_p, число силовских p-подгупп группы G, $p = 3, 5$. Имеем $N_3 \equiv 1 \pmod 3$ и $N_3 \,|\, 5$ (число силовских p-подгрупп делит индекс силовской p-подгруппы). Отсюда следует, что $N_3 = 1$. Следовательно, силовская 3-подгруппа единственна и значит нормальна. Обозначим ее через G_3. Поскольку порядок группы G_3 равен квадрату простого числа – $|G_3| = 3^2$, она абелева.

Аналогично получаем $N_5 \equiv 1 \pmod 5$ и $N_5 \,|\, 9$, откуда $N_5 = 1$, и следовательно, силовская 5-подгруппа единственна, а значит нормальна. Обозначим ее через G_5. Поскольку $|G_5| = 5$, группа G_5 изоморфна $\mathbb{Z}_5$, и поэтому абелева.

Из того, что $G_3 \cap G_5 = \{e\}$ и нормальности подгрупп G_3 и G_5, следует, что группа G является прямым произведением $G = G_3 \times G_5$. Из абелевости сомножителей вытекает абелевость группы G.

Поскольку G абелева имеются только две возможности – либо G изоморфна $\mathbb{Z}_9 \oplus \mathbb{Z}_5$, либо – $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$. $\square$

Задача 0.31. Показать, что если каждый элемент группы, отличный от единицы, имеет порядок 2, то группа абелева.

Решение. Пусть $a \neq b$ – два произвольных элемента группы, отличных от единицы. Тогда $a^2 = e = b^2$, откуда $a = a^{-1}$, $b = b^{-1}$, поэтому $ab \neq e$, и, значит, тоже имеет порядок 2, т.е. $(ab)^2 = e$. Следовательно,

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba,$$

т.е. $ab = ba$. $\square$

Например, пользуясь этим утверждением, легко показать, что группа порядка 4 абелева и изоморфна либо $\mathbb{Z}_4$, либо $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. В частности, четверная группа Клейна V_4 изоморфна группе $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, поскольку не является циклической (в ней все три отличных от e элемента имеют порядок 2).

Задача 0.32. Доказать, что группа порядка $2p$, где p – простое число большее 2, либо изоморфна циклической группе $\mathbb{Z}_{2p} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_p$, либо диэдральной группе D_p.

Доказательство. Поскольку порядок группы делится на простые числа 2 и p, в ней имеется элемент a порядка p и элемент b порядка 2, причем $b \notin \langle\, a \,\rangle = \langle\, a \,\rangle_p$, поскольку в циклической группе $\langle\, a \,\rangle_p$ все элементы, кроме e имеют порядок $p > 2$. Нетрудно видеть, что среди $2p$ элементов

$$e, a, a^2, \ldots, a^{p-1}, b, ab, a^2b, \ldots, a^{p-1}b$$

нет равных, поэтому группа порождается элементами a и b. Индекс подгруппы $\langle\, a \,\rangle_p$ равен двум, поэтому она нормальна. Следовательно, $bab = bab^{-1} = i_b(a) \in \langle\, a \,\rangle_p$ и, значит, $i_b(a) = a^m$ для некоторого $m \in 1, \ldots, p-1$. Если $m = 1$, то $ab = ba$ и этот элемент имеет порядок $2p$, т.е. наша группа изоморфна циклической группе $\mathbb{Z}_{2p}$. Если же $m > 1$, то применив внутренний автоморфизм i_b к равенству $i_b(a) = a^m$ получим

$$i_b(i_b(a)) = i_b(a^m) = (i_b(a))^m = (a^m)^m = a^{m^2}.$$

Но $i_b(i_b(a)) = i_{b^2}(a) = i_e(a) = a$, поэтому $a = a^{m^2}$, откуда $a^{m^2-1} = e$. Следовательно $m^2 - 1 = (m-1)(m+1)$ делится на p, и поскольку $1 \le m \le p-1$, либо $m = 1$, либо $m = p-1$. При $m = 1$ получаем рассмотренный выше случай, а при $m = p-1$ имеем $bab = a^{p-1} = a^{-1}$, и тогда $G \cong D_p$, см. задачу ниже. □

Задача 0.33. Предположим, что $G = \langle\, a, b \,\rangle$ имеет порядок $2n$, порядки элементов a и b равны n и 2 соответственно, и $bab = a^{-1}$. Тогда $G \cong D_n$.

Решение. Ясно, что $b \notin \langle\, a \,\rangle_n$, и легко видеть, что $G = \langle\, a \,\rangle_n \cdot \langle\, b \,\rangle_2$. Кроме того, подгруппа $\langle\, a \,\rangle_n$ нормальна так как ее индекс равен двум и $\langle\, a \,\rangle_n \cap \langle\, b \,\rangle_2 = \{e\}$. Поэтому наша группа является внутренним полупрямым произведением этих подгрупп, причем точно таким же каким является D_n, если под $a, b \in D_n$ понимать те образующие диэдральной группы, которые были введены нами выше при определении этой группы (a – поворот комплексной плоскости против часовой стрелки на угол $2\pi/n$, b – сопряжение). □

Задача 0.34. Найти классы сопряженных элементов в группе D_n.

Решение. Мы знаем, что D_n порождается элементами $a, b \in D_n$, такими, что $a^n = e = b^2$ и $bab = a^{-1}$. Последнее равенство записывается в виде $i_b(a) = a^{-1}$, поскольку $b = b^{-1}$. Имеем $ba^kb = i_b(a^k) = (i_b(a))^k = (a^{-1})^k = a^{-k}$, т.е. $ba^k = a^{-k}b$. В частности, $ba^{-1} = ab$.

$$i_{a^m b}(a^k) = i_{a^m}(i_b(a^k)) = i_{a^m}(a^{-k}) = a^m a^{-k} a^{-m} = a^{-k} = a^{n-k}.$$

Таким образом, a^k и a^{-k} лежат в одном классе и других элементов там нет. Если n нечетно, получаем классы $\{e\}$, $\{a, a^{n-1}\}$, $\{a^2, a^{n-2}\}, \ldots, \{a^{\frac{n-1}{2}}, a^{\frac{n+1}{2}}\}$. Число этих классов равно $\frac{n+1}{2}$. При четном n имеем классы
$\{e\}, \{a, a^{n-1}\}, \{a^2, a^{n-2}\}, \ldots, \{a^{\frac{n}{2}-1}, a^{\frac{n}{2}+1}\}, \{a^{n/2}\}$, число которых равно $\frac{n}{2} + 1$.

Далее,
$i_b(b) = bbb^{-1} = b$,
$i_a(b) = aba^{-1} = aab = a^2b$,
$i_a(a^kb) = i_a(a^k)i_a(b) = a^ka^2b = a^{k+2}b$,
$i_{a^2}(b) = i_a(i_a(b)) = i_a(a^2b) = i_a(a^2)i_a(b) = a^2i_a(b) = a^4b$,
$i_{a^m}(b) = a^{2m}b$.
Из этих равенств видно, что b и $a^{2m}b$ сопряжены, поэтому при нечетном n все элементы вида a^kb принадлежат одному классу сопряженных элементов. При четном n элементы ab и $a^{2m+1}b$ сопряжены, но не сопряжены с b и получается два класса сопряженных элементов. Сказанное следует из вычислений:

$i_b(a^kb) = ba^k = a^{-k}b$,
$i_{a^m}(a^kb) = i_{a^m}(a^k)i_{a^m}(b) = a^k i_{a^m}(b) = a^{2m+k}b$,
$i_{a^m b}(a^kb) = i_{a^m}(i_b(a^kb)) = i_{a^m}(a^{-k}b) = a^{2m-k}b$.

Итак общее число классов сопряженных элементов равно $\frac{n+1}{2} + 1 = \frac{n+3}{2}$ при нечетном n, и равно $\frac{n}{2} + 3 = \frac{n+6}{2}$ при четном n. $\square$