Лекция 3. Теорема Лагранжа, классы сопряженности, нормальные подгруппы, полупрямое произведение.

Теорема 1. Пусть G — конечная группа. Для любой точки $x \in X$ верно $|G| = |Gx| \cdot |G_x|$.

Доказательство. Пусть $|Gx| = a, |G_x| = b$. Обозначим элементы орбиты $Gx = \{g_1x, g_2x, \dots, g_ax\}$, где $g_1, \dots, g_a$ — элементы G , можно считать, что $g_1 = e$. Занумеруем также элементы стабилизатора $G_x = \{h_1, h_2 \dots h_b\}$, опять же можно считать, что $h_1 = e$. Тогда любой элемент $g \in G$ однозначно представим в виде $g = g_i h_j$.

Действительно, так как $gx \in Gx$ значит $gx = g_i x$, тем самым мы однозначно определили g_i . После этого $h_j = g_i^{-1} g$.

Значит, $|G| = a \cdot b = |Gx| \cdot |G_x|$. ■

Определение 1. Группа G действует на себе *умножением слева* по формуле $(g, x) \mapsto gx$.

Полезно *ограничить* это действие на подгруппу $H \subset G$, то есть рассмотреть действие H на G по формуле $(h, x) \mapsto hx$. Орбиты для этого действия — множества Hg — называются *правыми классами смежности*.

Так как $hx = x$ означает, что $h = e$, то стабилизатор любой точки тривиален, значит все орбиты состоят из $|H|$ элементов. Следовательно $|G| = |H| \cdot |G/H|$. Мы доказали следующую теорему:

Теорема 2 (Лагранж). Пусть G — конечная группа, H — подгруппа. Тогда $|H|$ делит порядок $|G|$.

Предложение 3 (Следствие). Пусть G — конечная группа. Тогда для любого элемента $g \in G$ порядок g делит $|G|$. В частности $g^{|G|} = e$

Доказательство. Пусть порядок g равен d . Тогда элементы $e, g, g^2, \dots, g^{d-1}$ образуют подгруппу, порядок этой подгруппы равен d . По теореме Лагранжа получаем, что d делит $|G|$, что и требовалось доказать. Также $g^{|G|} = (g^d)^{|G|/d} = e$. ■

Предложение 4 (Малая теорема Ферма). Если p — простое число, $a \in \mathbb{Z}$, и $\text{НОД}(a, p) = 1$, то $a^{p-1} - 1$ делится на p .

Доказательство Возьмем $G = \mathbb{Z}_p^*$, тогда заменив a на его остаток по модулю p имеем $a^{p-1} = 1$ в группе $\mathbb{Z}_p^*$, значит $a^{p-1} \equiv 1 \pmod{p}$. ■

Предложение 5 (Теорема Эйлера). Обозначим $|\mathbb{Z}_n^*| = \varphi(n)$. Тогда если $\text{НОД}(a, n) = 1$, то $a^{\varphi(n)} - 1$ делится на n

Доказывается аналогично прошлому пункту.

Помимо действия умножения слева можно определить действие справа.

Определение 2. Группа G действует на себе *умножением справа* по формуле $(g, x) \mapsto xg^{-1}$.

Определение 3. Группа G действует на себе сопряжениями по формуле $(g, x) \mapsto gxg^{-1}$.

Орбиты для действия группы на себе сопряжениями называются *классами сопряженности*.

Надо проверить корректность определения, т.е. что получается действительно действие:

$$g_1g_2(x)g_2^{-1}g_1^{-1} = g_1g_2(x)(g_1g_2)^{-1}, \text{ так как } (g_1g_2)^{-1} = g_2^{-1}g_1^{-1}.$$

Замечание. Сопряжение является автоморфизмом (изоморфизмом с собой) группы так как

$$gxyg^{-1} = gxg^{-1}gyg^{-1}$$

Примеры

1. Если группа G коммутативная, то каждый класс сопряженности состоит из одного элемента.

2. В группе S_3 есть три класса сопряженности: e ; $(1, 2)$, $(1, 3)$, $(2, 3)$; $(1, 2, 3)$, $(1, 3, 2)$.

Предложение 6. Пусть $\sigma = (i_1, i_2, \dots, i_k)(j_1, j_2, \dots, j_l) \dots$ и α произвольная перестановка. Тогда $\alpha\sigma\alpha^{-1} = (\alpha(i_1), \alpha(i_2), \dots, \alpha(i_k))(\alpha(j_1), \alpha(j_2), \dots, \alpha(j_l)) \dots$

Предложение 7 (Следствие). Две перестановки сопряжены в группе S_n тогда и только тогда, когда они имеют одинаковую циклическую структуру, т.е. их разложения в произведения независимых циклов для любого k содержат одинаковое число циклов длины k .

3. Пусть G — группа движений $\mathbb{R}^3$, S_π симметрия относительно плоскости π , g — некоторое движение. Тогда $gS_\pi g^{-1} = S_{g(\pi)}$ является симметрией относительно плоскости $g(\pi)$.

Пусть $R_{l,\varphi}$ — поворот вокруг оси l на угол φ , g — некоторое движение. Тогда $gR_{l,\varphi}g^{-1} = R_{g(l),\varphi}$ является поворотом поворот вокруг оси $g(l)$ на угол φ .

Вообще, сопряжение движения посредством g означает ортогональную замену базиса (и, возможно, смену начала координат) в $\mathbb{R}^3$, поэтому движение будет переходить в движение такого же типа, но геометрические данные изменяются посредством g .

4. Пусть G — группа матриц $GL(n, C)$. Тогда две матрицы A, B сопряжены если и только если у них одинаковые жордановы нормальны формы.

По аналогии с векторными пространствами естественно хотеть ввести структуру умножения на классах смежности. Для этого надо чтобы $g_1H \cdot g_2H = g_1g_2H$. Т.е. для любых $h_1, h_2 \in H$ существует $h \in H$ такой $g_1h_1g_2h_2 = g_1g_2h$. Значит $g_2^{-1}h_1g_2 = hh_2^{-1}$. Т.е. нужно чтобы $gHg^{-1} \subset H$.

Определение 4. Подгруппа $N \subset G$ называется *нормальной* (иногда говорят *инвариантной*) если для любого $g \in G$ верно $gNg^{-1} = N$. Это иногда записывают $N \triangleleft G$.

Свойства. 1. Если $N \triangleleft G$, то N является объединением каких-то классов сопряженности.

2. Если $N \triangleleft G$, то левые и правые смежные классы совпадают $gN = Ng$.

Доказательство. Возьмем произвольный элемент $gn \in gN$ левого класса смежности. Тогда $gn = gng^{-1}g \in Ng$ так как $gng^{-1} \in N$ в силу нормальности N . ■

Оба этих свойства можно было взять в качестве определения нормальной подгруппы.

Примеры

0. Если группа G коммутативная, то любая подгруппа является нормальной.

1. Пусть $G = S_3$. По теореме Лагранжа подгруппы могут быть только из 1, 2, 3 или 6 элементов. Подгруппа из одного элемента это $\{e\}$, она всегда нормальна, подгруппа из 6 элементов это вся G , она тоже нормальная. Подгруппа из двух элементов может состоять только из e и какая-то транспозиция, такая подгруппа не является нормальной так как сопряжением мы можем перевести транспозицию в любую другую. Подгруппа из трех элементов это только $\{e, (1, 2, 3), (1, 3, 2)\}$, она нормальная, так как состоит из полных классов сопряженности.

2. Пусть $G = A \times B$. Тогда подгруппы $\{(a, e)\} \simeq A$ и $\{(e, b)\} \simeq B$ являются нормальными.

Предложение 8. Если $N \triangleleft G$, то смежные классы по N образуют группу. Эта группа называется *факторгруппой* и обозначается G/N .

Операция умножения вводится по формуле

$$g_1N \cdot g_2N = g_1g_2N,$$

надо проверять корректность определения, и она следует из нормальности N , как было показано выше.

Примеры

1. Пусть группа $G = \mathbb{Z}$. Подгруппы имеют вид $H = n\mathbb{Z}$. Смежные классы имеют вид $a+n\mathbb{Z}$, т.е. состоят из чисел которые дают один остаток при делении на n . Складываются эти множества так же как и соответствующие остатки, поэтому факторгруппа $\mathbb{Z}/n\mathbb{Z}$ изоморфна $\mathbb{Z}_n$.

2. Пусть $G = V$ векторное пространство, $H = U$ векторное подпространство. Тогда факторгруппа V/U называется факторпространством, элементам являются множества вида $v+U$, геометрически можно о них думать о плоскостях (размерности $\dim U$) параллельных U . Сложение определено по формуле $(v_1+U) + (v_2+U) = v_1+v_2+U$. есть также операция умножения на скаляр.

Если на V есть скалярное произведение, то факторпространство можно отождествить с ортогональным дополнением к U в V .

3. Пусть $G = A \times B$. Тогда классы смежности G по подгруппе $\{(a, e)\} \simeq A$ имеют вид (A, y) , где $y \in B$, их произведение сводится к умножение второй координаты. Значит $G/A \simeq B$.

4. На плоскости рассмотрим решетку из параллелограммов общего вида (т.е. решетка не разбивается ни на прямоугольники ни на ромбы). Пусть G — группа движений переводящих эту решетку в себя.

Движения получаются двух видов: трансляции относительно векторов решетки и центральные симметрии относительно точек *половинной* решетки (т.е. вершин параллелограммов, середин сторон параллелограммов и центров параллелограммов). Группа трансляций (обозначим ее T) порождена сдвигами на порождающие вектора решетки (обозначим их e_1, e_2) и изоморфна $\mathbb{Z}^2$, общий элемент ее выглядит как

$$t_{n_1, n_2} : x \mapsto x + n_1 e_1 + n_2 e_2, \quad n_1, n_2 \in \mathbb{Z}.$$

Общая центральная симметрия сохраняющая решетку имеет вид

$$s_{m_1, m_2} : x \mapsto -x + m_1 e_1 + m_2 e_2, \quad m_1, m_2 \in \mathbb{Z}.$$

Подгруппа T является нормальной. Это видно из вычисления:

$$\begin{aligned} s_{m_1, m_2} t_{n_1, n_2} s_{m_1, m_2}(x) &= s_{m_1, m_2} t_{n_1, n_2}(-x + m_1 e_1 + m_2 e_2) = \\ &= s_{m_1, m_2}(-x + (n_1 + m_1)e_1 + (n_2 + m_2)e_2) = x - n_1 e_1 - n_2 e_2 = t_{-n_1, -n_2}(x) \end{aligned}$$

В группе G есть ровно два смежных класса по T — это сама T и все центральные симметрии. Поэтому фактор группа G/T состоит из двух элементов, значит изоморфна C_2 .

Эту группу C_2 можно явно указать внутри G . Например рассмотрим подгруппу $G_0 = \{e, s_{0,0}\}$ движений сохраняющих начало координат. Однако она не будет нормальной. Поэтому G не изоморфно произведению G_0 и T . Но на самом деле она изоморфна полупрямому произведению.

Определение 5. Пусть даны две группы A, B и гомоморфизм ϕ из группы A в группу автоморфизмов B . Т.е. для любого элемента $a \in A$ есть биекция $\phi_a : B \rightarrow B$ такая, что

$$\phi_a(b_1 b_2) = \phi_a(b_1) \phi_a(b_2), \quad \text{и} \quad \phi_{a_1}(\phi_{a_2}(b)) = \phi_{a_1 a_2}(b)$$

для любых $a, a_1, a_2 \in A$ и $b_1, b_2, b \in B$. *Полупрямым произведением* $A \ltimes B$ называется группа элементами которой являются всевозможные пары $\{(a, b)\} \in A \times B$ с умножением

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, \phi_{a_2^{-1}}(b_1) b_2).$$

Замечание. В полупрямом произведении $A \ltimes B$ есть подгруппы изоморфные A и B , но только подгруппа изоморфная B является нормальной. Смысл отображения ϕ_a — это сопряжение B посредством элемента $a \in A$.

Замечание. Условия на ϕ_a можно сформулировать, как то, что группа A действует на группе B автоморфизмами.

Примеры

1. Пусть $\phi_a(b) = b$, для любых $a \in A$, $b \in B$. Тогда полупрямое произведение $A \ltimes B$ изоморфно прямому произведению $A \times B$
2. Группа G симметрий общей параллелограммной решетки изоморфна полупрямому произведению $G_0 \ltimes T$. Группа G_0 действует на T следующим образом $\phi_e(t_{n_1, n_2}) = t_{n_1, n_2}$, $\phi_{s_0}(t_{n_1, n_2}) = t_{-n_1, -n_2}$.

Домашнее задание

Решения задач 2, 3, 4а надо прислать до начала лекции 27 февраля. Остальные задачи надо прислать или принести до начала лекции 6 марта. Помимо письменной сдачи надо быть готовым ответить на вопросы по решениям.

Упражнение 1. Проверьте корректность определения полупрямого произведения (то есть, проверьте, что формула действительно задает группу).

Задача 2. а) Пусть G — группа движений сохраняющих правильный тетраэдр. Докажите, что действие G на множестве вершин тетраэдра задает изоморфизм G и S_4 . Опишите геометрически (как вращения, симметрии или зеркальные повороты) все перестановки. Найдите классы сопряженности.

б) Пусть G_0 это подгруппа собственных движений сохраняющих правильный тетраэдр. Является ли она нормальной? Найдите классы сопряженности в G_0 .

Задача 3. а) Через D_{nh} обозначим группу симметрий прямоугольной призмы с основанием правильный n угольник. Найдите порядок группы D_{nh} .

Другое описание группы D_{nh} — группа движений трехмерного пространства, сохраняющих правильный n -угольник лежащий в плоскости XOY .

б) Можно ли представить D_{3h} в виде произведения (прямого или полупрямого?). Изоморфны ли группы D_{3h} и D_6 ?

Задача 4. а) Пусть G — группа симметрий прямоугольной (но не квадратной) решетки на плоскости, T — подгруппа состоящая из трансляций. Докажите, что T является нормальной подгруппой в G . Найдите факторгруппу G/T . Представьте G в виде полупрямого произведения.

б)* Найдите классы сопряженности в G .