Лекция 9

Рассмотрим действие группы G на множестве всех подгрупп в группе G сопряжениями. В самом деле, легко убедиться, что если $H \subset G$ – подгруппа, то gHg^{-1} также подгруппа.

Определение 1. Стабилизатор подгруппы H при данном действии называется *нормализатором* H в G и обозначается $N_G(H)$.

Лемма 1. *1) $N_G(H)$ – подгруппа в G,*
2) $H \subseteq N_G(H)$,
3) H нормальна в $N_G(H)$,
4) Если H нормальна в K, где K – подгруппа G, то $K \subset N_G(H)$.

Доказательство. 1) По определению, $N_G(H)$ – стабилизатор, а значит, подгруппа в G.
2) Если $h \in H$, то $hHh^{-1} = H$. Значит, $h \in N_G(H)$.
3) При $g \in N_G(H)$ имеем $gHg^{-1} = H$, это доказывает нормальность H в $N_G(H)$.
4) Если $H \triangleleft K$, то для любого $k \in K$ выполнено $kHk^{-1} = H$, то есть

$$k \in St(H) = N_G(H).$$

□

Пусть $|G| = p^k m$. Обозначим через n_p число силовских p-подгрупп в группе G.

Теорема 1 (Третья теорема Силова)**.**
1) n_p сравнимо с 1 по модулю p,
2) n_p делит m.

Доказательство. 1) Пусть S – одна из силовских p-подгрупп. Рассмотрим действие S на множестве M силовских p-подгрупп сопряжениями. То есть $s \cdot S' = sS's^{-1}$. Пусть $Orb(S')$ – некая орбита. Тогда $|Orb(S')| \cdot |St(S')| = |S| = p^k$. Значит, $|Orb(S')| = p^l$. Среди орбит есть $Orb(S)$, которая состоит только из одной подгруппы S, таким образом, $|Orb(S)| = 1$.

Пусть $S' \neq S$, допустим, что $|Orb(S')| = 1$. Тогда для любых $s \in S, s' \in S'$ имеем $ss's^{-1} \in S'$. Следовательно, $S \subseteq N_G(S')$. Заметим, что $N_G(S')$ – это подгруппа в G, а значит, $|N_G(S')| = p^u v|$, где $u \leq k$ и $(p, v) = 1$. Так как $S \subseteq N_G(S')$, $u = k$. Значит, S – силовская p-подгруппа в $N_G(S')$. С другой стороны S' – силовская p-подгруппа в $N_G(S')$. Значит, S и S' сопряжены в $N_G(S')$. Но S' нормальна в $N_G(S')$, а значит, сопрягая S' элементами $N_G(S')$ мы не получим дргой подгруппы. ПРотиворечие. Значит, не существует такой $S' \neq S$, что $|Orb(S')| = 1$.

Итак, множество M силовских p-подгрупп состоит из орбит, одна из них имеет порядок 1, а остальные имеют порядки p^l, где $l \neq 0$. Следовательно, $n_p = |M|$ имеет остаток 1 при делении на p.

2) Рассмотрим действие группы G на множестве L всех подгрупп в G. То есть $g \cdot H = gHg^{-1}$. По второй теореме Силова все силовские p-подгруппы образуют одну орбиту $\mathcal{O}$. Пусть S – одна из силовских p-подгрупп. Тогда

$$|G| = |\mathcal{O}| \cdot |St(S)| = n_p \cdot |St(S)|.$$

Отсюда $|G| = p^k m$ делится на n_p. Так как НОД$(n_p, p) = 1$, получаем m делится на n_p. □

Пример 1. *Группа порядка 15 обязательно изоморфна $\mathbb{Z}_{15}$. Докажем это. Применим третью теорему Силова к $p = 3$ и $p = 5$ в нашей группе. Получим*

$$\begin{cases} n_3 \equiv 1 (\operatorname{mod} 3); \\ n_3 \mid 5. \end{cases}$$

Отсюда $n_3 = 1$. А также

$$\begin{cases} n_5 \equiv 1 (\operatorname{mod} 5); \\ n_5 \mid 3. \end{cases}$$

Отсюда $n_5 = 1$. Это значит, что в нашей группе есть 2 подгруппы $H_3 \cong \mathbb{Z}_3$ и $H_5 \cong \mathbb{Z}_5$, причём они обе нормальны (так как являются единственными силовскими подгруппами). Пересечение H_3 и H_5 – это только $\{e\}$, так как любой неединичный элемент в H_3 имеет порядок 3, а любой неединичный элемент в H_5 имеет порядок 5. Докажем, что $\langle H_3, H_5 \rangle = G$. В самом деле, пусть $\langle H_3, H_5 \rangle = L \subseteq G$. Тогда по теореме Лагранжа $|L|$ делится на 3 и на 5. То есть $|L|$ делится на 15. Следовательно, $L = G$. Получаем, что для подгрупп H_3 и H_5 выполнены условия внутреннего прямого произведения, что означает

$$G \cong H_3 \times H_5 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{15}.$$

Определение 2. Пусть x и y – элементы группы G. *Коммутатором* элементов x и y называется элемент

$$[x, y] = xyx^{-1}y^{-1}.$$

Лемма 2. *$[x, y] = e$ тогда и только тогда, когда элементы x и y перестановочны (то есть $xy = yx$).*

Доказательство.

$$xy = yx \;\Leftrightarrow\; xyx^{-1} = y \;\Leftrightarrow\; xyx^{-1}y^{-1} = e.$$

□

Замечание 1. Обратный элемент к коммутатору является коммутатором. В самом деле:

$$[x, y]^{-1} = (xyx^{-1}y^{-1})^{-1} = yxy^{-1}x^{-1} = [y, x].$$

Определение 3. *Коммутант* группы G – это подгруппа, порожденная всеми коммутаторами пар элементов из G. Коммутант группы G обозначается G' или $[G, G]$.

Лемма 3. *Коммутант состоит из произведений коммутаторов.*

Доказательство. По определению, G' состоит из произведений коммутаторов и обратных к ним. Но, так как обратный к коммутатору – коммутатор, G' состоит из произведения коммутаторов. □

Лемма 4. *$G' = \{e\}$ тогда и только тогда, когда G коммутативна.*

Доказательство. Если G коммутативна, то все коммутаторы равны e, и значит, коммутант также равен $\{e\}$.

Если же G не абелева, то найдутся два элемента x и y такие, что $xy \neq yx$. Тогда $[x, y] \neq e \in G'$. □

Лемма 5. *Коммутант G' – нормальная подгруппа в G.*

Доказательство. Заметим, что

$$g[x,y]g^{-1} = gxyx^{-1}y^{-1}g^{-1} = gxg^{-1}gyg^{-1}gx^{-1}g^{-1}gy^{-1}g^{-1} = [gxg^{-1}, gyg^{-1}].$$

Отсюда

$$g[x_1,y_1][x_2,y_2]\dots[x_n,y_n]g^{-1} = g[x_1,y_1]g^{-1}g[x_2,y_2]g^{-1}\dots g[x_n,y_n]g^{-1} = \\ = [gx_1g^{-1}, gy_1g^{-1}][gx_2g^{-1}, gy_2g^{-1}]\dots[gx_ng^{-1}, gy_ng^{-1}].$$

Таким образом, если сопрячь с помощью g элемент коммутанта (то есть произведение коммутаторов), то получится снова элемент коммутанта. Таким образом, коммутант – нормальная подгруппа. □

Лемма 6. *Группа G/G' коммутативна.*

Доказательство. Рассмотрим коммутатор двух произвольных элементов из G/G':

$$[gG', hG'] = gG' \cdot hG' \cdot (gG')^{-1} \cdot (hG')^{-1} = [g,h]G' = G'.$$

То есть коммутатор любых элементов из G/G' равен единице группы G/G'. Значит, G/G' – абелева группа. □

Теорема 2. *а) Пусть H – подгруппа в G и $G' \subseteq H$. Тогда H – нормальная подгруппа и G/H – абелева группа.*

б) Если $G \rhd H$ и группа G/H – абелева группа то $G' \subset H$.

Доказательство. а) Пусть $g \in G$, $h \in H$. Тогда $ghg^{-1} = [g,h]h \in H$. Значит, $G \rhd H$.

Рассмотрим коммутатор двух произвольных элементов из G/H:

$$[g_1H, g_2H] = g_1H \cdot g_2H \cdot (g_1H)^{-1} \cdot (g_2H)^{-1} = [g_1,g_2]H = H.$$

Значит, $(G/H)' = \{e\}$, то есть G/H – коммутативная группа.

б) Рассмотрим коммутатор двух произвольных элементов из G/H:

$$[g_1H, g_2H] = g_1H \cdot g_2H \cdot (g_1H)^{-1} \cdot (g_2H)^{-1} = [g_1,g_2]H.$$

Так как G/H – абелева группа, $[g_1H, g_2H] = H$. Получаем $[g_1,g_2]H = H$, следовательно, $[g_1,g_2] \in H$. Поскольку коммутаторы порождают G', выполняется $G' \subset H$. □

Можно рассмотреть кратные коммутанты: $G^{(2)} = (G')'$, $G^{(3)} = \left(G^{(2)}\right)'$, … , $G^{(n)} = \left(G^{(n-1)}\right)'$, …

Определение 4. Группа G называется *разрешимой*, если существует $n \in \mathbb{N}$ такое, что $G^{(n)} = \{e\}$.

Число n называется *ступенью (степенью)* разрешимости G.

Пример 2. *Группа G разрешима ступени 1 тогда и только тогда, когда G абелева.*

Пример 3.

- *Группа S_2 разрешима ступени 1.*
- *Группа S_3 разрешима ступени 2: $S_3' = A_3$, $A_3' = \{\mathrm{id}\}$.*
- *Группа S_4 разрешима ступени 3: $S_4' = A_4$, $A_4' = V_4$, $V_4' = \{\mathrm{id}\}$.*
- *Группа S_n при $n \geq 5$ не разрешима. Действительно, $S_n' = A_n$, $A_n' = A_n$ (будет показано позже).*

Лемма 7. *Подгруппа разрешимой группы разрешима.*

Доказательство. Пусть H – подгруппа G. Тогда $H' \subset G'$, $H'' \subset G''$ и т.д. Значит, $H^{(n)} \subset G^{(n)} = \{e\}$. □