Группы - I

Часть 1. Теорема Жордана–Гельдера

Определение 1.1. Группа G называется простой, если она не имеет нетривиальных нормальных подгрупп.

Примеры 1.2. 1. Коммутативная группа G проста $\iff G = \mathbb{Z}/p\mathbb{Z}$, где p — простое;
2. Знакопеременная группа A_n проста при $n = 2$ и $n \geqslant 5$.

Определение 1.3. Башня подгрупп $G = G_0 \supset G_1 \supset \cdots \supset G_{m-1} \supset G_m = 1$, называется простой, если $\forall s \leqslant m$ группа G_s нормальна в G_{s-1} и группа G_{s-1}/G_s проста.

Определение 1.4. Одна башня подгрупп называется уплотнением другой башни, если последовательность подгрупп из второй башни является подпоследовательностью последовательности подгрупп первой башни.

Лемма 1.5. *Всякая нормальная башня конечной группы может быть уплотнена до простой башни.*

Доказательство: Рассмотрим нормальную башню с максимальным количеством нетривиальных факторов, являющуюся уплотнением исходной. Если бы один из факторов G_{s-1}/G_s в этой башне не являлся простой группой, то башню можно было бы уплотнить следующим образом. Выберем нетривиальную нормальную подгруппу $H \triangleleft G_{s-1}/G_s$ и положим $G'_i = G_i$ при $i \leqslant s-1$, $G'_i = G_{i-1}$ при $i \geqslant s+1$ и обозначим через G'_s прообраз подгруппы H в G_{s-1} относительно канонического эпиморфизма $G_{s-1} \to G_{s-1}/G_s$. Ясно, что новая башня нормальна, является уплотнением предыдущей, и имеет больше нетривиальных факторов, что противоречит выбору предыдущей башни. Следовательно, предыдущая башня являлась простой. $\square$

Возникает вопрос, насколько единственна простая башня данной группы. Ясно, что ответ отрицательный: например, $\mathbb{Z}/6\mathbb{Z} \supset 2\mathbb{Z}/6\mathbb{Z} \supset 1$ и $\mathbb{Z}/6\mathbb{Z} \supset 3\mathbb{Z}/6\mathbb{Z} \supset 1$ — различные простые башни группы $\mathbb{Z}/6\mathbb{Z}$. Однако видно, что хоть башни и различны, но множества факторгрупп, встречающихся в них, совпадают.

Теорема 1.6. *Если $G = G_0 \supset G_1 \supset \cdots \supset G_{m-1} \supset G_m = 1$ и $G = G'_0 \supset G'_1 \supset \cdots \supset G'_{n-1} \supset G'_n = 1$ — простые башни группы G, в которых все включения строгие, то $m = n$ и последовательности их факторов отличаются перестановкой.*

Начнем с леммы.

Лемма 1.7. *Пусть $G_2 \triangleleft G_1 \subset G$ и $G'_2 \triangleleft G'_1 \subset G$. Тогда* $\dfrac{G_2(G_1 \cap G'_1)}{G_2(G_1 \cap G'_2)} \cong \dfrac{(G_1 \cap G'_1)G'_2}{(G_2 \cap G'_1)G'_2}$.

Доказательство: рассмотрим сначала левую дробь. Ясно, что $G_1 \cap G'_2 \subset G_1 \cap G'_1 \subset G_1 \subset N_{G_2}$, поэтому произведения групп в ее числителе и знаменателе являются подгруппами в G. Кроме того, $(g_2 g_{11})(h_2 g_{12})(g_2 g_{11})^{-1} = g_2(g_{11} h_2 g_{11}^{-1})(g_{11} g_{12} g_{11}^{-1}) g_2 \in G_2 G_2 (G_1 \cap G'_2) G_2 = G_2(G_1 \cap G'_2)$, где $g_{11} \in G_1 \cap G'_1$, $g_{12} \in G_1 \cap G'_2$ и $g_2, h_2 \in G_2$, поэтому знаменатель является нормальной подгруппой в числителе и левая факторгруппа имеет смысл. Рассмотрим теперь композицию гомоморфизмов

$$f : G_1 \cap G'_1 \to G_2(G_1 \cap G'_1) \to \frac{G_2(G_1 \cap G'_1)}{G_2(G_1 \cap G'_2)}.$$

Так как $G_2(G_1 \cap G'_2)(G_1 \cap G'_1) = G_2(G_1 \cap G'_1)$, то f сюръективен. Далее, $\operatorname{Ker} f = (G_1 \cap G'_1) \cap G_2(G_1 \cap G'_2)$. Покажем, что

$$(G_1 \cap G'_1) \cap G_2(G_1 \cap G'_2) = (G_2 \cap G'_1)(G_1 \cap G'_2).$$

Действительно, легко видеть, что каждый из сомножителей правой части лежит в каждом из сомножителей левой части, откуда получаем включение $\supset$. Возьмем теперь произвольный элемент в левой части. Его можно записать в виде $g_2 g_{12}$, где $g_2 \in G_2$, $g_{12} \in G_1 \cap G'_2$, причем $g_2 g_{12} \in G_1 \cap G'_1 \subset G'_1$. Следовательно, $g_2 = (g_2 g_{12}) g_{12}^{-1} \in G'_1(G_1 \cap G'_2) \subset G'_1 G'_2 \subset G'_1$, значит $g_2 \in G_2 \cap G'_1$ и $g_2 g_{12} \in (G_2 \cap G'_1)(G_1 \cap G'_2)$. Тем самым доказано включение $\subset$, а стало быть и равенство.

Получаем $\dfrac{G_2(G_1\cap G_1')}{G_2(G_1\cap G_2')}\cong\dfrac{G_1\cap G_1'}{(G_2\cap G_1')(G_1\cap G_2')}$. Аналогично $\dfrac{(G_1\cap G_1')G_2'}{(G_2\cap G_1')G_2'}\cong\dfrac{G_1\cap G_1'}{(G_1\cap G_2')(G_2\cap G_1')}$. Остается заметить, что $G_1\cap G_2'\subset G_1\cap G_1'\subset N_{G_2}\cap N_{G_1'}\subset N_{G_2\cap G_1'}$, поэтому $(G_1\cap G_2')(G_2\cap G_1')\cong(G_2\cap G_1')(G_1\cap G_2')$. □

Доказательство теоремы: положив $G_{ij}:=G_{i+1}(G_i\cap G_j')$, получаем уплотнение $G=G_0=G_{00}\supset G_{01}\supset\cdots\supset G_{0n}=G_1=G_{10}\supset G_{11}\supset\cdots\supset G_{m-1,n}=1$ первой башни. Аналогично, положив $G_{ij}':=(G_j\cap G_i')G_{i+1}'$, получаем уплотнение $G=G_0'=G_{00}'\supset G_{01}'\supset\cdots\supset G_{0m}'=G_1'=G_{10}'\supset G_{11}'\supset\cdots\supset G_{n-1,m}'=1$ второй башни. Из леммы следует, что

$$\frac{G_{ij}}{G_{i,j+1}}=\frac{G_{i+1}(G_j'\cap G_i)}{G_{i+1}(G_{j+1}'\cap G_i)}\cong\frac{(G_j\cap G_i')G_{i+1}'}{(G_{j+1}\cap G_i')G_{i+1}'}=\frac{G_{ij}'}{G_{i,j+1}'},$$

следовательно факторы в этих башнях попарно изоморфны. Остается заметить, что так как исходные башни были простыми, то наборы факторов в исходных башнях и их уплотнениях совпадают. □

Простая башня группы также называется рядом Жордана–Гельдера или композиционным рядом.

Часть 2. Разрешимые и нильпотентные группы

Напомним, что группа G называется разрешимой, если она обладает абелевой башней подгрупп, то есть башней $G=G_0\supset G_1\supset\cdots\supset G_{m-1}\supset G_m=1$, в которой $\forall s\leqslant m$ $G_s\triangleleft G_{s-1}$ и группа G_{s-1}/G_s абелева. Иначе говоря, группа разрешима, если все простые факторы в ее ряде Жордана–Гельдера коммутативны.

Пусть G — произвольная группа, а $H_1,H_2\subset G$ — ее подгруппы. Обозначим через $[H_1,H_2]$ подгруппу в G, порожденную всеми коммутаторами $[h_1,h_2]:=h_1h_2h_1^{-1}h_2^{-1}$, где $h_1\in H_1$, $h_2\in H_2$. В частности, группа $[G,G]$ называется коммутантом группы G и обозначается G'.

Лемма 2.1. *Если подгруппы H_1 и H_2 нормальны в G, то подгруппа $[H_1,H_2]\subset G$ тоже нормальна.*

Доказательство: $g[h_1,h_2]g^{-1}=gh_1h_2h_1^{-1}h_2^{-1}g^{-1}=(gh_1g^{-1})(gh_2g^{-1})(gh_1^{-1}g^{-1})(gh_1^{-1}g^{-1})=[gh_1g^{-1},gh_2g^{-1}]$. □

Лемма 2.2. *Коммутант всякой группы G является нормальной подгруппой, а факторгруппа G/G' абелева. Более того, если $f:G\to A$ — гомоморфизм группы G в абелеву группу A, то $G'\subset\operatorname{Ker}f$.*

Доказательство: во-первых, коммутант нормален в силу предыдущей леммы. Во-вторых, ясно что в факторгруппе G/G' всякий коммутатор равен 1, значит группа G/G' — абелева. Наконец, если A — произвольная абелева группа, а $f:G\to A$ — гомоморфизм, то $f([g_1,g_2])=f(g_1g_2g_1^{-1}g_2^{-1})=f(g_1)f(g_2)f(g_1)^{-1}f(g_2)^{-1}=[f(g_1),f(g_2)]=1$, значит $G'\subset\operatorname{Ker}f$. □

Пусть теперь G — произвольная группа и рассмотрим следующую башню ее подгрупп: $G^{(0)}=G$, $G^{(1)}=[G,G]=G'$, … , $G^{(s)}=[G^{(s-1)},G^{(s-1)}]=(G^{(s-1)})'$.

Теорема 2.3. *Группа G разрешима $\Longleftrightarrow$ $G^{(s)}=1$ для некоторого s.*

Доказательство: Из предыдущей леммы следует, что башня из коммутантов является абелевой башней, откуда вытекает ($\Longleftarrow$). Пусть теперь $G=G_0\supset G_1\supset\cdots\supset G_{m-1}\supset G_m=1$ — произвольная абелева башня. Покажем, что $G^{(s)}\subset G_s$ для всех s. Воспользуемся индукцией по s. Случай $s=0$ очевиден. Теперь предположим, что $G^{(s-1)}\subset G_{s-1}$ и рассмотрим композицию гомоморфизмов $G^{(s-1)}\to G_{s-1}\to G_{s-1}/G_s$. Так как G_{s-1}/G_s — абелева группа, то $G^{(s)}$ лежит в ядре композиции, следовательно $G^{(s)}\subset G_s$. □

Определение 2.4. Башня подгрупп $G=G_0\supset G_1\supset\cdots\supset G_{m-1}\supset G_m=1$ называется центральным рядом, если $\forall s\leqslant m$ группа G_s нормальна в G, и G_{s-1}/G_s лежит в центре группы G/G_s.

Определение 2.5. Группа G называется нильпотентной, если она обладает конечным центральным рядом.

Примеры 2.6. 1. Коммутативная группа нильпотентна;

2. если G — p-группа (т.е. $|G|=p^n$), то G — нильпотентна (доказывается индукцией по n, используя тот факт, что центр p-группы всегда нетривиален).

Определение 2.7. Последовательность групп $Z_0G = G$, $Z_1G = [G, G]$, ..., $Z_sG = [Z_{s-1}G, G]$ называется нижним центральным рядом группы G.

Последовательность групп $Z^0G = 1$, $Z^1G = Z(G)$, $Z^sG = \phi_{s-1}^{-1}(Z(G/Z^{s-1}G))$, где $\phi_{s-1} : G \to G/Z^{s-1}G$ — канонический эпиморфизм, называется верхним центральным рядом группы G.

Лемма 2.8. *Построенные ряды являются центральными.*

Доказательство: начнем с нижнего центрального ряда. Во-первых, ясно что Z_sG — подгруппа в G, порожденная элементами вида $[\dots[[g_1, g_2], g_3], \dots, g_s]$, следовательно $Z_sG \subset Z_{s-1}G$. Во-вторых, из леммы 2.1 следует, что группа Z_sG нормальна в G. Наконец, коммутатор любого элемента из $Z_{s-1}G$ с любым элементом из G лежит в Z_sG, поэтому группа $Z_{s-1}G/Z_sG$ содержится в центре группы G/Z_sG. Значит нижний центральный ряд действительно является центральным.

Что касается верхнего центрального ряда, то здесь надо проверить лишь то, что $Z^sG \triangleleft G$. Воспользуемся индукцией. Случай $s = 0$ очевиден. Предположим теперь, что $Z^{s-1}G \triangleleft G$ и пусть $g \in G$, $h \in Z^sG$. Тогда, так как $\phi_{s-1}(h)$ лежит в центре группы $G/Z^{s-1}G$, то $\phi_{s-1}(ghg^{-1}) = \phi_{s-1}(g)\phi_{s-1}(h)\phi_{s-1}(g)^{-1} = \phi_{s-1}(h)$, значит $\phi_{s-1}(ghg^{-1})$ тоже лежит в центре группы $G/Z^{s-1}G$, следовательно $ghg^{-1} \in Z^sG$ и $Z^sG \triangleleft G$. $\square$

Будем говорить, что верхний (нижний) центральный ряд группы G обрывается, если для некоторого s имеем $Z^sG = G$ (соотв. $Z_sG = 1$). Минимальное такое s называется длиной соответствующего центрального ряда.

Теорема 2.9. *Следующие условия эквивалентны: (i) группа G нильпотентна; (ii) верхний центральный ряд группы G обрывается; (iii) нижний центральный ряд группы G обрывается.*

Часть 3. Силовские подгруппы

Пусть p — простое число. Группа H называется p-группой, если ее порядок есть степень числа p. Пусть теперь G — конечная группа. Подгруппа $H \subset G$ называется силовской p-подгруппой, если H — p-группа и ее индекс не делится на p. Иначе говоря, если $|G| = p^k m$ и $(p, m) = 1$, то H — силовская, если $|H| = p^k$.

Теорема 3.1. *Всякая конечная группа G имеет силовскую p-подгруппу для любого p.*

Доказательство: индукция по $n = |G|$. Если $p \not| n$, то $H = 1$ и доказывать нечего. Пусть $p|n$. По формуле классов имеем $n = (Z : 1) + \sum_{x \in G \setminus Z}(G : G_x)$, значит, либо $p|(Z : 1)$, либо найдется $x \in G$, такое что $p \not|(G : G_x)$. Во втором случае имеем $|G_x| < |G|$, значит, по предположению индукции G_x имеет силовскую p-подгруппу, которая будет силовской и в G. В первом же случае выберем в абелевой группе Z подгруппу Z' порядка p и рассмотрим $G' = G/Z'$ (Z' нормальна, так как лежит в центре). Если $H' \subset G'$ — силовская p-подгруппа, то ее прообраз в G тоже является силовской p-подгруппой. $\square$

Теорема 3.2. *(i) Всякая p-подгруппа $H \subset G$ содержится в силовской p-подгруппе. (ii) Все силовские p-подгруппы в G сопряжены. (iii) Количество силовских p-подгрупп в G равно 1 по модулю p.*

Доказательство: рассмотрим действие группы G сопряжениями на множестве всех своих p-подгрупп.

(i) Пусть $H \subset G$ — p-подгруппа, P — силовская p-подгруппа, а S — орбита P под действием G. Тогда $|S| = (G : N_P)$, где N_P — нормализатор P. Но ясно, что $P \subset N_P$, поэтому $|S|$ взаимно прост с p. Рассмотрим теперь действие H на S. Порядок S равен сумме длин орбит. С другой стороны, всякая орбита группы H имеет порядок равный p^s, следовательно, найдется орбита порядка 1. Пусть она состоит из группы P'. Тогда $H \subset N_{P'}$, следовательно, $HP' \subset G$ — подгруппа и, так как $HP'/P' \cong H/(H \cap P')$, то HP' является p-группой. Но так как $P' \subset HP'$ и P' силовская, то $HP' = P'$, значит, $H \subset P'$.

(ii) Заметим, что в (i) мы доказали даже более сильное утверждение. А именно, если H — p-подгруппа, а P — силовская p-подгруппа, то H лежит в силовской подгруппе, сопряженной к P. Если H — сама силовская, то получаем, что H и P сопряжены.

(iii) Рассмотрим действие силовской группы P на множестве всех силовских групп. Длина любой орбиты — это степень p, причем орбита группы P' состоит из одной точки $\iff P \subset N_{P'}$, но как показано в (i) из этого следует $P' = P$. Таким образом, длина всех орбит, кроме орбиты $\{ P \}$ делится на p. $\square$

Замечание 3.3. Так как множество всех силовских p-подгрупп — орбита группы G, то их количество равно индексу нормализатора силовской p-подгруппы P, следовательно делит $(G : P) = |G|/p^n$.