Л.12

4.2. Степенные и коммутаторные тождества. Абелевы многообразия

Мы будем говорить, что из набора тождеств $\{w_i = 1\}$ *следует* тождество $v = 1$, если оно выполняется в каждой группе, в которой выполняются все тождества $\{w_i = 1\}$. Два набора тождеств мы называем *эквивалентными*, если они задают одно и то же многообразие, то есть каждое из тождеств первого набора следует из тождеств второго набора и наоборот.

Тождество $w(x_1, x_2, \ldots) = 1$ мы называем *коммутаторным*, если каждая буква входит в слово $w(x_1, x_2, \ldots)$ с суммарной степенью ноль. Тождество вида $x^k = 1$, где x — одна из букв алфавита, называется *степенным*. Отметим, что произвольный набор степенных тождеств $\{x_i^{k_i}\}$ эквивалентен одному степенному тождеству $x^n = 1$, где число n есть наибольший общий делитель чисел $\{n_i\}$.

Утверждение 4.2. *Любой набор тождеств эквивалентен не более чем счётному набору тождеств* $\{w_1 = 1,\ w_2 = 1, \ldots\}$ *в счётном алфавите* $\{x_1, x_2, \ldots\}$*. Причём первое тождество* $w_1 = 1$ *имеет вид* $x_1^n = 1$ *(то есть является степенным), а все остальные тождества* $w_2 = 1$, $w_3 = 1, \ldots$ *являются коммутаторными.*

Доказательство. Поскольку любое тождество включает в себя лишь конечное число букв и от названия этих букв ничего не зависит, это тождество эквивалентно некоторому тождеству в фиксированном счётном алфавите $\{x_1, x_2, \ldots\}$. Но в этом счётном алфавите существует лишь счётное число различных тождеств. Следовательно, любой набор тождеств эквивалентен счётному набору тождеств в счётном алфавите $\{x_1, x_2, \ldots\}$.

Рассмотрим теперь произвольное такое тождество $u(x_1, \ldots, x_n) = 1$. Пусть $k_1, \ldots, k_n$ суть суммы показателей степеней в слове u при буквах $x_1, \ldots, x_n$ соответственно. Тогда тождество $u(x_1, \ldots, x_n) = 1$ можно переписать в виде

$$x_1^{k_1} \ldots x_n^{k_n} u' = 1, \quad \text{где } u' \text{ имеет вид } x_n^{-k_n} \ldots x_1^{-k_1} u \text{ и является коммутаторным словом.} \qquad (*)$$

Последовательно подставляя единицы в тождество $(*)$ вместо всех букв кроме x_i, мы получаем степенные следствия тождества $u = 1$:

$$x_1^{k_1} = 1,\ \ldots,\ x_n^{k_n} = 1. \qquad (**)$$

Из тождеств $(*)$ и $(**)$ мы получаем коммутаторное следствие $u' = 1$ тождества $u = 1$. Осталось заметить, что из тождеств $(**)$ и $u' = 1$ очевидным образом следует исходное тождество $u = 1$. Таким образом, всякое тождество эквивалентно некоторому набору степенных и коммутаторных тождеств. Значит, и всякий набор тождеств эквивалентен набору степенных и коммутаторных тождеств. Для завершения доказательства осталось вспомнить, что каждый набор степенных тождеств эквивалентен одному степенному тождеству.

Нетрудно сообразить, что если многообразие $\mathcal{V}$ задано набором тождеств $x^n = 1$, $w_1 = 1$, $w_2 = 1, \ldots$, где тождества $w_i = 1$ являются коммутаторными, то число n зависит только от многообразия $\mathcal{V}$ и может быть инвариантно определено как наибольшее число k такое, что $\mathbb{Z}_k \in \mathcal{V}$. Это число называют *экспонентой многообразия* $\mathcal{V}$. (Если $n = 0$, то принято говорить, что экспонента бесконечна.)

Следствие 4.2. *Множество всех многообразий абелевых групп находится во взаимно однозначном соответствии с множеством* $\mathbb{N} \cup \{\infty\}$*. Это соответствие сопоставляет многообразию его экспоненту. Обратное соответствие сопоставляет числу* n *многообразие, задаваемое парой тождеств* $[x, y] = 1$ *и* $x^n = 1$*. Пересечению многообразий при этой биекции соответствует наибольший общий делитель натуральных чисел.*

Доказательство этого следствия мы оставляем в качестве упражнения.

4.3. Относительно свободные группы

Важную роль в нашем доказательстве теоремы Биркгофа играла группа F. Напомним, что эта группа лежала в некотором классе групп $\mathcal{K}$ и обладала такой системой образующих Y, что каждое отображение из множества Y в любую группу G из класса $\mathcal{K}$ продолжалось (единственным образом) до гомоморфизма $F \to G$. Группы, обладающие этим свойством, называют *свободными в классе* $\mathcal{K}$. Множество порождающих Y, фигурирующее в этом определении, называют *свободным базисом* (или *свободными образующими*) свободной группы F. Мощность базиса называют *рангом* свободной группы F. Группа F называется *относительно свободной*, если она свободна в некотором классе групп.

Ранг относительно свободной группы может быть произвольным кардиналом. Следующее простое утверждение показывает, что свободная в классе $\mathcal{K}$ группа однозначно определяется своим рангом.

Утверждение 4.3.1. *Две свободные в некотором классе* $\mathcal{K}$ *группы одинаковых рангов изоморфны.*

Доказательство. Пусть $F, G \in \mathcal{K}$ — две свободные в $\mathcal{K}$ группы, X и Y — их свободные базисы и $|X| = |Y|$. Рассмотрим какую-нибудь биекцию $f\colon X \to Y$. По определению свободности эта биекция продолжается до гомоморфизма $\widehat{f}\colon F \to G$. Обратная биекция $f^{-1}\colon Y \to X$ продолжается до гомоморфизма $\widehat{f^{-1}}\colon G \to F$. Осталось заметить, что композиции $\widehat{f^{-1}} \circ \widehat{f}: F \to F$ и $\widehat{f} \circ \widehat{f^{-1}}: G \to G$ являются тождественными отображениями, поскольку они оставляют на месте каждый из порождающих.

Из доказательства теоремы Биркгофа можно усмотреть, что каждое многообразие обладает свободными группами любых рангов. Правда, это доказательство не даёт явного описания таких групп. На самом деле, для многих важных многообразий явное описание свободных групп известно. Например, свободные группы в многообразии всех абелевых групп — это знакомые нам свободные абелевы группы. Свободная группа ранга k в многообразии абелевых групп экспоненты n — это прямая сумма k экземпляров группы $\mathbb{Z}_n$. В книге [Нейм69] читатель может найти вполне удовлетворительное описание свободных нильпотентных групп. Свободные разрешимые группы устроены сложнее, но всё же поддаются изучению.

Важнейшим многообразием групп является, разумеется, многообразие всех групп. Свободные группы этого многообразия называют *абсолютно свободными*, или просто *свободными группами*. Мы будем весьма подробно изучать абсолютно свободные группы во второй части этой книги, а сейчас мы ограничимся тем, что дадим их явное описание.

Пусть X — некоторый алфавит, $x_1, \ldots, x_n \in X$ и $\varepsilon_1, \ldots, \varepsilon_n \in \{\pm 1\}$. Слово $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_n^{\varepsilon_n}$ в алфавите $X \cup X^{-1}$ называется *несократимым*, если оно не содержит подслов вида xx^{-1} и $x^{-1}x$ ни для какого $x \in X$. *Несократимой формой* произвольного слова u в алфавите $X \cup X^{-1}$ называют несократимое слово, получающееся из u вычёркиванием подслов вида xx^{-1} и $x^{-1}x$. Очевидно, что каждое слово имеет несократимую форму (возможно, пустую). Чуть менее очевиден следующий факт, доказательство которого мы оставляем в качестве упражнения.

Лемма 4.3. *Несократимая форма каждого слова единственна, то есть не зависит от того, в каком порядке выполняются вычёркивания.*

Произведением двух несократимых слов $u = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_n^{\varepsilon_n}$ и $v = y_1^{\delta_1} y_2^{\delta_2} \ldots y_m^{\delta_m}$ называют несократимую форму uv слова
$$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_n^{\varepsilon_n} y_1^{\delta_1} y_2^{\delta_2} \ldots y_m^{\delta_m},$$
получающегося приписыванием слова v к слову u. Например произведением слов
$$x^3y^2x^{-1} = xxxyyx^{-1} \quad \text{и} \quad xy^{-2}x^{-1}y^3 = xy^{-1}y^{-1}x^{-1}yyy \quad \text{будет слово} \quad x^2y^3 = xxyyy.$$

Утверждение 4.3.2. *Множество несократимых слов $F(X)$ в произвольном алфавите X образует группу относительно введённого выше умножения. Единицей этой группы является пустое слово, а обратным к слову $x_1^{\varepsilon_1} \ldots x_n^{\varepsilon_n}$ служит слово $x_n^{-\varepsilon_n} \ldots x_1^{-\varepsilon_1}$. Группа $F(X)$ является абсолютно свободной группой со свободным базисом X.*

Доказательство. Доказательство того, что $F(X)$ является группой, мы оставляем в качестве упражнения. Докажем свободность этой группы. Пусть $f: X \to G$ — произвольное отображение из множества X в произвольную группу G. Мы хотим показать, что это отображение продолжается до гомоморфизма $\widehat{f}: F(X) \to G$. Отображение $\widehat{f}$ определяется естественным образом:
$$\widehat{f}(x_1^{\varepsilon_1} \ldots x_n^{\varepsilon_n}) = f(x_1)^{\varepsilon_1} \ldots f(x_n)^{\varepsilon_n}.$$
Покажем, что $\widehat{f}$ — гомоморфизм. Действительно, пусть имеются два несократимых слова $u = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_n^{\varepsilon_n}$ и $v = y_1^{\delta_1} y_2^{\delta_2} \ldots y_m^{\delta_m}$. Тогда их произведение имеет вид
$$uv = x_1^{\varepsilon_1} \ldots x_{n-k}^{\varepsilon_{n-k}} y_{k+1}^{\delta_{k+1}} \ldots y_m^{\delta_m},$$
где k — это наибольшее число, для которого $y_k = x_{n-k+1}$ и $\delta_k = \varepsilon_{n-k+1}$. Но сокращение подряд идущих взаимно обратных элементов возможно и в группе G, поэтому
$$\widehat{f}(u)\widehat{f}(v) = f(x_1)^{\varepsilon_1} \ldots f(x_n)^{\varepsilon_n} f(y_1)^{\delta_1} \ldots f(y_m)^{\delta_m} = f(x_1)^{\varepsilon_1} \ldots f(x_{n-k})^{\varepsilon_{n-k}} f(y_{k+1})^{\delta_{k+1}} \ldots f(y_m)^{\delta_m},$$
что и доказывает гомоморфность отображения $\widehat{f}$.

4.4. Порождение многообразий

Пусть $\mathcal{K}$ — произвольный класс групп. *Многообразием, порождённым классом* $\mathcal{K}$, называют наименьшее многообразие $\mathbf{var}\,\mathcal{K}$, содержащее класс $\mathcal{K}$. Другими словами, $\mathbf{var}\,\mathcal{K}$ состоит из всех групп, в которых выполнены все тождества, выполненные в классе $\mathcal{K}$ (то есть во всех группах из класса $\mathcal{K}$). Согласно теореме Биркгофа каждая группа многообразия $\mathbf{var}\,\mathcal{K}$ получается из групп, лежащих в $\mathcal{K}$, с помощью операций декартова произведения, перехода к подгруппам и перехода к факторгруппам. Отметим, что на самом деле при доказательстве теоремы Биркгофа мы установили несколько более сильный факт.

Утверждение 4.4.1. *Многообразие* $\mathbf{var}\,\mathcal{K}$, *порождённое классом групп* $\mathcal{K}$, *состоит из факторгрупп подгрупп декартовых произведений групп из* $\mathcal{K}$.

Итак, у нас есть два способа задать многообразие: можно либо написать набор тождеств, определяющих это многообразие, либо указать набор групп, порождающих это многообразие. Эта ситуация аналогична той, которая возникает, например, в линейной алгебре: подпространство векторного пространства можно задать либо системой уравнений, либо набором векторов, порождающих это подпространство. Для каждого многообразия $\mathcal{V}$ возникает естественный вопрос: Какое минимальное число групп порождает многообразие $\mathcal{V}$, и какое минимальное число тождеств задаёт $\mathcal{V}$? Другими словами, продолжая аналогию с линейной алгеброй, какая у $\mathcal{V}$ «размерность» и какая «коразмерность»? Ответ на первую половину вопроса прост: всякое неединичное многообразие «одномерно», то есть порождается одной группой.

Утверждение 4.4.2. *Каждое многообразие порождается своей свободной группой счётного ранга.*

Доказательство. Пусть $F = F_{\mathcal{V}}(x_1, x_2, \ldots)$ — свободная группа многообразия $\mathcal{V}$ со свободным базисом $\{x_1, x_2, \ldots\}$. Если слово w в алфавите $\{x_1^{\pm1}, x_2^{\pm1}, \ldots\}$ не является тождеством многообразия $\mathcal{V}$, то оно не выполнено и в группе F (поскольку имеется гомоморфизм из F в произвольную группу $G \in \mathcal{V}$, переводящий x_i в произвольные элементы $g_i \in G$). Значит, в многообразии $\mathbf{var}\,F \subseteq \mathcal{V}$ выполняются только те тождества в алфавите $\{x_1, x_2, \ldots\}$, которые выполнены в $\mathcal{V}$. Для завершения доказательства остаётся вспомнить, что согласно утверждению 4.2 всякое тождество эквивалентно некоторому тождеству в указанном алфавите.

На первый взгляд может показаться, что и «коразмерность» многообразия не может быть больше единицы.

Неверная теорема. *Каждое многообразие задаётся одним тождеством.*

Неверное доказательство. Пусть

$$w_1(x_1, \ldots, x_n) = 1,\ w_2(x_1, \ldots, x_n) = 1,\ \ldots,\ w_l(x_1, \ldots, x_n) = 1 \qquad (*)$$

— минимальный набор тождеств, задающий многообразие $\mathcal{V}$. Допустим, что $l \geqslant 2$. Рассмотрим новые буквы $y_1, \ldots, y_n$ и тождество

$$w_1(x_1, \ldots, x_n)w_2(y_1, \ldots, y_n) = 1, \qquad (**)$$

которое очевидным образом следует из первых двух тождеств набора $(*)$. Но, с другой стороны, первые два тождества набора $(*)$ являются следствиями тождества $(**)$ (они получаются из этого тождества подстановкой единиц вместо части переменных и переобозначениями). Например, пара тождеств, задающих многообразие абелевых групп периода n (пример 4.1.3), эквивалентна одному тождеству $[x, y]z^n = 1$.

Значит, многообразие $\mathcal{V}$ можно задать $l - 1$ тождеством

$$w_1(x_1, \ldots, x_n)w_2(y_1, \ldots, y_n) = 1,\ w_3(x_1, \ldots, x_n) = 1,\ \ldots,\ w_l(x_1, \ldots, x_n) = 1.$$

Это противоречит минимальности числа l и завершает доказательство.

Читатель, который не видит ошибки в этом рассуждении, может не огорчаться — чуть позже мы обсудим, почему неверно это «доказательство». Гораздо труднее доказать, что неверна сама «теорема».

4.5. Проблема конечной базируемости. Тождества нильпотентных групп

Ошибка в приведённом выше рассуждении состоит в том, что мы заранее предполагали, что многообразие задаётся конечным набором тождеств. На самом деле мы доказали такой факт:

Утверждение 4.5. *Если многообразие задаётся конечным набором тождеств, то оно задаётся одним тождеством.*

Многообразия, о которых идёт речь в этом утверждении, называют *конечно базируемыми*. Долгое время было неизвестно, существуют ли не конечно базируемые многообразия групп. Первые примеры таких многообразий были построены А.Ю. Ольшанским, С.И. Адяном и М.Р. Воном-Ли (см. [Ольш89] или [Адян75]). В силу утверждения 4.4.2 наличие таких многообразий означает, что существует группа, тождества которой не следуют ни из какого конечного числа тождеств этой группы. Следствие 4.2 показывает, что такая группа не может быть абелевой. Следующая теорема показывает, что такая группа не может быть и нильпотентной.

Теорема 4.5. *Многообразие, порождённое нильпотентной группой, конечно базируемо.*

Доказательство. Пусть G — нильпотентная группа ступени s.
Шаг 1. Докажем сперва, что все тождества группы G следуют из некоторого набора тождеств этой группы, каждое из которых включает в себя не более $s + 1$ буквы.

Заметим, что по модулю тождества $[x_1,\ldots,x_{s+1}]=1$, выполненного в G, каждое тождество можно записать в виде

$$c_1c_2\ldots c_n=1,\quad \text{где } c_1,\ldots,c_n \text{ — коммутаторы длины не больше } s \text{ от букв алфавита } X\ . \tag{1}$$

Скажем, что тождество $c_1c_2\ldots c_n=1$, записанное в виде (1), меньше тождества $c_1'c_2'\ldots c_n'=1$, также записанного в виде (1), если либо минимум длин коммутаторов $c_1,c_2,\ldots,c_n$ больше минимума длин коммутаторов $c_1',c_2',\ldots,c_n'$, либо эти минимумы равны, но число коммутаторов минимальной длины среди $c_1,c_2,\ldots,c_n$ меньше числа коммутаторов минимальной длины среди $c_1',c_2',\ldots,c_n'$. Ясно, что всякая последовательность тождеств вида (1), каждое из которых меньше предыдущего, конечна. Следовательно, нам достаточно показать, что всякое тождество $u=1$ группы G следует из некоторого набора тождеств этой группы, каждое из которых либо меньше тождества $u=1$, либо зависит от не более чем $s+1$ переменной.

Рассмотрим некоторое тождество

$$c_1c_2\ldots c_n=1. \tag{2}$$

Можно считать, что коммутатор $c_1=[x_1,\ldots,x_m]$, где $x_i\in X$ — (не обязательно различные) буквы, имеет здесь минимальную длину $m\leqslant s$. Этого всегда можно достичь, не увеличивая тождество (в смысле введённого порядка), поскольку при перестановке коммутаторов возникают коммутаторы большей длины. Подставив в тождество (2) единицы вместо всех букв, кроме $x_1,\ldots,x_m$, мы получим новое тождество

$$c_1d_1\ldots d_k=1 \tag{3}$$

от m переменных. Частное

$$d_k^{-1}\ldots d_1^{-1}c_2\ldots c_n=1 \tag{4}$$

тождеств (2) и (3) будет меньше тождества (2), поскольку сократится коммутатор c_1. Осталось заметить, что тождество (2) очевидным образом следует из тождеств (3) и (4), одно из которых имеет не более s переменных, а другое меньше тождества (2).

Шаг 2. Осталось показать, что все тождества $w_1(x_1,\ldots,x_{s+1})=1$, $w_2(x_1,\ldots,x_{s+1})=1$, … группы G от не более чем $s+1$ переменной следуют из конечного числа таких тождеств.

Возьмём свободную нильпотентную ступени s группу F со свободным базисом $x_1,\ldots,x_{s+1}$. Рассмотрим подгруппу $H=\langle w_1(x_1,\ldots,x_{s+1}),w_2(x_1,\ldots,x_{s+1}),\ldots\rangle$ группы F, порождённую левыми частями тождеств группы G. (На самом деле нетрудно сообразить, что H совпадает с множеством $\{w_1,w_2,\ldots\}$.) Подгруппа H, как и всякая подгруппа конечно порождённой нильпотентной группы, конечно порождена. Пусть

$$H=\langle u_1(x_1,\ldots,x_{s+1}),\ldots,u_l(x_1,\ldots,x_{s+1})\rangle\,.$$

Тогда все тождества $w_1=1$, $w_2=1$, … следуют из тождеств $u_1=1$, …, $u_l=1$ и тождества нильпотентности $[x_1,\ldots,x_{s+1}]=1$ (проверьте).

Среди разрешимых групп встречаются не конечно базируемые. А вот всякая метабелева группа обладает конечным базисом тождеств. Доказательство этого результата Д.Е. Коэна основано на одном обобщении теоремы Гильберта о базисе. Весьма нетривиальная теорема А.Н. Красильникова утверждает, что и все группы с нильпотентным коммутантом обладают конечным базисом тождеств. Верны ли аналогичные утверждения для полициклических групп или для линейных групп — неизвестно. Ещё об одном, быть может, самом интересном, факте, касающимся конечной базируемости, мы поговорим в следующем параграфе.

4.6. Тождества конечных групп

Теорема Оутс–Пауэлла. *Каждая конечная группа имеет конечный базис тождеств.*

Не очень сложное доказательство этой теоремы, принадлежащее Ковачу и Ньюману, читатель может найти в книге [Нейм69]. В этих лекциях мы, следуя в основном [БаОл88], проследим за некоторыми из основных этапов этого доказательства на примере простейшей неабелевой конечной группы S_3. Материал этого параграфа можно рассматривать как приблизительный рецепт нахождения базиса тождеств конечной группы.

Итак, пусть нам дана конечная группа G и мы хотим найти базис её тождеств, то есть написать такой конечный набор тождеств, выполненных в группе G, чтобы все остальные тождества этой группы были следствиями написанных. Первое, что мы должны сделать, — это написать какие-нибудь тождества группы G. Причём написать настолько сильный набор тождеств, чтобы у нас возникло предположение, что все остальные тождества этой группы уже следуют из написанных. В случае группы S_3 нам в голову могут прийти, например, такие тождества:

$$x^6=1\quad \text{и}\quad [x^2,y^2]=1.$$

Допустим, что мы не можем придумать никаких других тождеств, которые выполнены в S_3, но не следуют из двух написанных. Например, тождество метабелевости является следствием второго из наших тождеств (покажите). У нас возникает гипотеза, что мы нашли базис тождеств группы S_3. Вопрос в том, как проверить эту гипотезу.

Утверждение 4.6.1. *Многообразие, порождённое конечной группой, **локально конечно**, то есть все конечно порождённые группы этого многообразия конечны.*

Доказательство. Согласно утверждению 4.4.1 нам достаточно показать, что любая конечно порождённая подгруппа H декартовой степени группы G конечна.

Поскольку существует лишь конечное число гомоморфизмов $H \to G$, среди проекций группы H на сомножители декартовой степени группы G имеется лишь конечное число различных. Обозначив это число буквой n, мы получаем очевидное вложение группы H в G^n и конечность группы H.

Это утверждение подсказывает, что мы должны проверить, является ли локально конечным многообразие $\mathcal{V}$, заданное написанным нами набором тождеств. В нашем случае ответ положительный, поскольку из второго тождества следует метабелевость, а из метабелевости и периодичности следует, как мы знаем, локальная конечность.

Важную роль в изучении тождеств конечных групп играет понятие критической группы. Группа G называется *критической*, если она не лежит в многообразии, порождённом всеми её собственными подгруппами и всеми её собственными факторгруппами. Примером критической группы может служить группа S_3, у которой все собственные подгруппы и факторгруппы абелевы, в отличие от неё самой.

Утверждение 4.6.2. *Локально конечное многообразие порождается множеством всех своих критических групп.*

Доказательство. Это утверждение почти очевидно. Дело в том, что всякое многообразие порождается своими конечно порождёнными группами (докажите), которые в данном случае конечны. А каждая конечная некритическая группа многообразия $\mathcal{W}$ лежит в многообразии, порождённом группами из $\mathcal{W}$ меньших порядков.

Следующее утверждение, которое мы оставляем без доказательства, является ключевым шагом в доказательстве теоремы Оутс–Пауэлла.

Утверждение 4.6.3. *Многообразие, порождённое конечной группой, содержит лишь конечное число критических групп.*

Посмотрим, каковы критические группы нашего многообразия $\mathcal{V}$. Каждая конечная группа H многообразия $\mathcal{V}$ представляет собой расширение нормальной подгруппы $N = \langle h^2\,;\, h \in H\rangle$ при помощи группы $L = H/N$. Из тождеств видно, что группа N является абелевой группой периода 3, то есть $N \simeq \mathbb{Z}_3^n$. А группа L имеет период 2, то есть $L \simeq \mathbb{Z}_2^l$. Нетрудно сообразить, что такое расширение всегда расщепляется (N и L являются силовскими подгруппами в H). Таким образом, $H = L \leftthreetimes N$.

Следующее простое утверждение позволяет сильно уменьшить число кандидатов на звание критической группы.

Утверждение 4.6.4. *Каждая критическая группа имеет наименьшую нетривиальную нормальную подгруппу.* Другими словами, *пересечение всех нетривиальных нормальных подгрупп критической группы нетривиально.**)

Доказательство. Если пресечение $\bigcap N_i$ нетривиальных нормальных подгрупп группы G тривиально, то естественное отображение группы G в декартово произведение групп G/N_i инъективно и, следовательно, $G \in \mathbf{var}\,\{G/N_i\}$.

Это означает, что если наша группа

$$H \simeq \mathbb{Z}_2^l \underset{\varphi}{\leftthreetimes} \mathbb{Z}_3^n$$

критическая, то либо $n = 0$ (а тогда l обязано быть единицей), либо представление $\varphi\colon \mathbb{Z}_2^l \to \operatorname{Aut}\mathbb{Z}_3^n \simeq \mathbf{GL}_n(\mathbb{Z}_3)$ является неприводимым, поскольку у всякого инвариантного подпространства есть инвариантное дополнение (по теореме Машке), и эти два дополнительных подпространства представляют собой тривиально пересекающиеся нормальные подгруппы. Нетрудно сообразить, что неприводимые представления группы $\mathbb{Z}_2^l$ над любым полем одномерны. Таким образом, $n = 1$. Но при $n > 0$ представление φ обязано быть точным, поскольку $\ker\varphi$ и $\mathbb{Z}_3^n$ представляют собой две тривиально пересекающиеся нормальные подгруппы группы H. Значит, $l \leqslant 1$.

В итоге мы получаем, что многообразие $\mathcal{V}$ содержит 3 критические группы: S_3, $\mathbb{Z}_3$ и $\mathbb{Z}_2$. Осталось заметить, что каждая из этих групп вкладывается в S_3 и, следовательно,

$$\mathcal{V} = \mathbf{var}\,\{S_3, \mathbb{Z}_3, \mathbb{Z}_2\} = \mathbf{var}\,S_3;$$

итак, мы доказали такое утверждение:

Утверждение 4.6.5. *Все тождества группы S_3 следуют из тождества $[x^2, y^2]z^6 = 1$.*

---

*) Группу, обладающую наименьшей нетривиальной нормальной подгруппой, называют ***монолитической***, а наименьшую нетривиальную нормальную подгруппы монолитической группы называют её ***монолитом***.