

гомоморфизма есть (нормальная) подгруппа индекса 2 и, следовательно, совпадает с  $H$ , т. е.  $H$  нормальна вопреки предположению. Это завершает доказательство.

Пусть  $G$  действует на множестве  $S$ . Тогда две орбиты группы  $G$  либо не пересекаются, либо совпадают. Действительно, если  $Gs_1$  и  $Gs_2$  — две орбиты с общим элементом  $s$ , то  $s = xs_1$  для некоторого  $x \in G$  и, следовательно,  $Gs = Gxs_1 = Gs_1$ . Аналогично  $Gs = Gs_2$ . Таким образом,  $S$  — объединение попарно не пересекающихся различных орбит, и мы можем записать

$$S = \bigcup_{i \in I} Gs_i \quad (Gs_i \text{ попарно не пересекаются}),$$

где  $I$  — некоторое множество индексов и  $s_i$  — элементы различных орбит. Если  $S$  конечно, это дает разложение порядка множества  $S$  в сумму порядков орбит, которое мы назовем *формулой разложения на орбиты*, а именно

$$\text{card}(S) = \sum_{i \in I} (G : Gs_i)$$

Пусть  $x, y$  — элементы группы (или монида)  $G$ . Они называются коммутирующими, если  $xy = yx$ . Если  $G$  — группа, то множество всех элементов  $x \in G$ , коммутирующих со всеми элементами  $G$ , есть подгруппа в  $G$ , которую мы назвали *центром* группы  $G$ . Пусть  $G$  действует на себе посредством сопряжения. Тогда элемент  $x$  лежит в центре в том и только в том случае, если орбита этого элемента совпадает с ним самим и, таким образом, состоит из одного элемента. Вообще, порядок орбиты элемента  $x$  равен индексу его нормализатора. Следовательно, в том случае, когда  $G$  — конечная группа, предыдущая формула принимает вид

$$(G : 1) = \sum_{x \in C} (G : G_x),$$

где  $C$  — множество представителей различных классов сопряженных элементов. Эта формула называется также *формулой классов*.

### § 6. Силовские подгруппы

Пусть  $p$  — простое число. Под  $p$ -группой мы понимаем конечную группу, порядок которой является степенью  $p$  (т. е. равен  $p^n$  для некоторого целого  $n \geq 0$ ). Пусть  $G$  — конечная группа и  $H$  — ее подгруппа. Мы называем  $H$   *$p$ -подгруппой* в  $G$ , если  $H$  —  $p$ -группа. Мы называем  $H$  *силовской  $p$ -подгруппой*, если порядок  $H$  есть  $p^n$  и если  $p^n$  — наибольшая степень  $p$ , делящая порядок  $G$ . Ниже мы

докажем, что такие подгруппы всегда существуют. Для этого нам понадобится лемма.

**Лемма.** *Пусть  $G$  — конечная абелева группа порядка  $m$  и  $p$  — простое число, делящее  $m$ . Тогда  $G$  содержит подгруппу порядка  $p$ .*

**Доказательство.** Докажем сначала по индукции, что если  $G$  имеет показатель  $n$ , то порядок группы  $G$  делит некоторую степень  $n$ . Пусть  $b \in G$ ,  $b \neq 1$ , и пусть  $H$  — циклическая подгруппа, порожденная  $b$ . Тогда порядок  $H$  делит  $n$ , так как  $b^n = 1$ . Далее,  $n$  есть показатель для  $G/H$ . Следовательно, порядок факторгруппы  $G/H$  делит, согласно индуктивному предположению, некоторую степень  $n$ , а в таком случае это справедливо и для порядка  $G$ , потому что

$$(G : 1) = (G : H)(H : 1).$$

Пусть порядок группы  $G$  делится на  $p$ . В силу только что доказанного в  $G$  существует элемент  $x$ , период которого делится на  $p$ . Пусть этот период равен  $ps$ , где  $s$  — некоторое целое число. Тогда  $x^s \neq 1$  и, очевидно, элемент  $x^s$  имеет период  $p$  и порождает подгруппу порядка  $p$ , что и требовалось доказать.

**Теорема 1.** *Пусть  $G$  — конечная группа и  $p$  — простое число, делящее ее порядок. Тогда в  $G$  существует силовская  $p$ -подгруппа.*

**Доказательство** проводится индукцией по порядку  $G$ . Если порядок простой, то наше утверждение очевидно. Предположим теперь, что теорема доказана для всех групп, порядок которых меньше порядка  $G$ . Если в  $G$  имеется собственная подгруппа  $H$ , индекс которой взаимно прост с  $p$ , то силовская  $p$ -подгруппа в  $H$  будет также силовской  $p$ -подгруппой в  $G$  и наше утверждение справедливо по индукции. Мы можем поэтому предположить, что у всякой собственной подгруппы индекс делится на  $p$ . Пусть теперь  $G$  действует на себе посредством сопряжений. Из формулы классов получаем

$$(G : 1) = (Z : 1) + \sum (G : G_x).$$

Здесь  $Z$  — центр  $G$  и член  $(Z : 1)$  соответствует орбитам, состоящим из одного элемента, т. е. как раз элементам из  $Z$ . Сумма справа берется по всем другим орбитам, поэтому каждый индекс  $(G : G_x) > 1$ , и по предположению делится на  $p$ . Так как  $p$  делит порядок  $G$ , отсюда следует, что  $p$  должно делить порядок  $Z$ ; в частности,  $G$  имеет нетривиальный центр.

Согласно лемме, в  $Z$  существует циклическая подгруппа  $H$ , порожденная элементом порядка  $p$ . Так как подгруппа  $H$  содержится

в  $Z$ , то она нормальна. Пусть  $f: G \rightarrow G/H$  — каноническое отображение. Если  $p^n$  — наибольшая степень  $p$ , делящая  $(G : 1)$ , то  $p^{n-1}$  делит порядок  $G/H$ . Пусть  $K'$  — силовская  $p$ -подгруппа в  $G/H$  (существующая по предположению индукции), и пусть  $K = f^{-1}(K')$ . Тогда  $K \trianglelefteq H$  и  $f$  отображает  $K$  на  $K'$ . Следовательно, имеет место изоморфизм  $K/H \approx K'$  и  $K$  имеет порядок  $p^{n-1}p = p^n$ , что и требовалось доказать.

**Теорема 2.** Для всякой конечной группы  $G$

- (i) каждая  $p$ -подгруппа содержится в некоторой силовской  $p$ -подгруппе;
- (ii) все силовские  $p$ -подгруппы сопряжены;
- (iii) число силовских  $p$ -подгрупп  $\equiv 1 \pmod{p}$ .

**Доказательство.** Все доказательства являются применением техники, связанной с формулой классов. Пусть  $S$  — множество силовских  $p$ -подгрупп в  $G$ . Тогда  $G$  действует на  $S$  посредством сопряжения. Пусть  $P$  — одна из силовских  $p$ -подгрупп. Группа изотропии  $G_P$  подгруппы  $P$  содержит  $P$ , и, следовательно, орбита подгруппы  $P$  (обозначим ее через  $S_0$ ) имеет порядок, взаимно простой с  $p$ . Пусть  $H$  —  $p$ -подгруппа порядка  $> 1$ . Тогда  $H$  действует посредством сопряжений на  $S_0$  и  $S_0$  распадается в объединение попарно не пересекающихся орбит относительно  $H$ . Так как порядок  $H$  есть степень  $p$ , то индекс любой ее собственной подгруппы делится на  $p$ , следовательно, хотя бы одна из  $H$ -орбит в  $S_0$  должна состоять только из одного элемента, а именно из некоторой силовской подгруппы  $P'$ . Тогда  $H$  содержится в нормализаторе  $P'$  и, следовательно,  $HP'$  есть подгруппа в  $G$ . Кроме того,  $P'$  нормальна в  $HP'$ . Так как

$$HP'/P' \approx H/(H \cap P'),$$

то порядок  $HP'/P'$  есть степень  $p$ , а потому и порядок  $HP'$  есть степень  $p$ . Так как  $P'$  — максимальная  $p$ -подгруппа в  $G$ , то мы должны иметь  $HP' = P'$  и, следовательно,  $H \subset P'$ , что доказывает (i).

В частности, рассмотрим случай, когда  $H$  — силовская  $p$ -подгруппа в  $G$ . Как мы показали,  $H$  содержится в некоторой подгруппе, сопряженной с  $P$ , и, значит, совпадает с ней (так как порядки их одинаковы). Это доказывает (ii). Наконец, возьмем  $H = P$ . Тогда одна из орбит относительно  $H$  содержит ровно один элемент (сама  $P$ ), а все другие орбиты имеют более одного элемента; в действительности порядки этих орбит делятся на  $p$ , поскольку они равны индексам собственных подгрупп в  $P$ . Это доказывает (iii).

**Теорема 3.** Пусть  $G$  — конечная  $p$ -группа. Тогда  $G$  разрешима. Если ее порядок  $> 1$ , то  $G$  имеет нетривиальный центр.

**Доказательство.** Первое утверждение следует из второго, так как если  $G$  имеет центр  $Z$  и мы по индукции имеем абелеву башню для  $G/Z$ , то мы можем поднять эту абелеву башню до  $G$ , показав тем самым, что  $G$  разрешима. Чтобы доказать второе утверждение, воспользуемся формулой классов

$$(G : 1) = \text{card}(Z) + \sum(G : G_x);$$

здесь сумма берется лишь по тем  $x$ , для которых  $(G : G_x) \neq 1$ . Очевидно,  $p$  делит  $(G : 1)$ , а также делит каждый член в сумме, так что порядок центра делится на  $p$ , что и требовалось доказать.

**Следствие.** Пусть  $G$  —  $p$ -группа, порядок которой отличен от 1. Тогда существует последовательность подгрупп

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \dots \subset G_n = G,$$

такая, что каждая подгруппа  $G_i$  нормальна в  $G$  и  $G_{i+1}/G_i$  — циклическая группа порядка  $p$ .

**Доказательство.** Так как центр группы  $G$  нетривиален, то в нем имеется элемент  $a \neq e$  порядка  $p$ . Пусть  $H$  — циклическая группа, порожденная  $a$ . По индукции, если  $G \neq H$ , то в факторгруппе  $G/H$  мы можем найти последовательность подгрупп, удовлетворяющую сформулированным требованиям. Взяв прообраз этой башни в  $G$ , получим искомую последовательность.

## § 7. Категории и функторы

Теперь, прежде чем идти дальше, нам будет удобно ввести новую терминологию. Мы уже встречались с объектами разного рода: множествами, моноидами, группами. Со многими другими мы еще встретимся, а для каждого такого рода объектов мы определяем специальный род отображений между ними (например, гомоморфизмы). Некоторые формальные свойства являются общими для всех них, а именно существование тождественных отображений объектов на себя и ассоциативность отображений, выполняемых одно за другим. Мы введем понятие категории, чтобы дать общее абстрактное описание таких ситуаций.

**Категория**  $\mathcal{A}$  включает в себя следующее: класс объектов  $\text{Ob}(\mathcal{A})$ ; для всяких двух объектов  $A, B \in \text{Ob}(\mathcal{A})$  множество  $\text{Mor}(A, B)$ , называемое множеством *морфизмов* объекта  $A$  в  $B$ ; для всяких трех объектов  $A, B, C \in \text{Ob}(\mathcal{A})$  закон композиции (т. е. отображение)

$$\text{Mor}(B, C) \times \text{Mor}(A, B) \rightarrow \text{Mor}(A, C).$$

При этом должны выполняться аксиомы: