в том смысле, что если два из этих индексов конечны, то конечен и третий и имеет место написанное равенство. Если порядок $(G:1)$ конечен, то он делится на порядок подгруппы H.

Более общо, пусть H, K — подгруппы в G, причем $H \supset K$. Пусть $\{x_i\}$ — множество представителей (левых) смежных классов H по K и $\{y_j\}$ — множество представителей смежных классов G по H. Тогда мы утверждаем, что $\{y_j x_i\}$ — множество представителей смежных классов группы G по K.

Чтобы доказать это, заметим, что

$$H = \bigcup_i x_i K,$$

$$G = \bigcup_j y_j H,$$

причем в обоих объединениях слагаемые попарно не пересекаются. Следовательно,

$$G = \bigcup_{i,\,j} y_j x_i K.$$

Мы должны показать, что в последнем объединении слагаемые также попарно не пересекаются, т. е. $y_j x_i$ представляют различные смежные классы. Предположим, что

$$y_j x_i K = y_{j'} x_{i'} K$$

для некоторой пары индексов (j, i) и (j', i'). Умножив на H справа и приняв во внимание, что x_i, $x_{i'}$ лежат в H, получим

$$y_j H = y_{j'} H,$$

откуда $y_j = y_{j'}$. Отсюда вытекает, что $x_i K = x_{i'} K$, а потому $x_i = x_{i'}$, что и требовалось показать.

Формула из предложения 1 может быть, следовательно, обобщена:

$$(G:K) = (G:H)(H:K),$$

причем понимать это нужно так: если два из трех индексов, входящих в формулу, конечны, то конечен и третий и имеет место написанное равенство.

§ 3. Циклические группы

Целые числа $\mathbf{Z}$ образуют аддитивную группу. Найдем ее подгруппы. Пусть H — подгруппа в $\mathbf{Z}$. Если H нетривиальна, то пусть a — ее наименьший положительный элемент. Мы утверждаем, что H состоит из всех элементов вида na, где $n \in \mathbf{Z}$. Чтобы доказать это, рассмотрим любой элемент $y \in H$. Существуют целые числа n, r, где $0 \leqslant r < a$, такие, что

$$y = na + r.$$

Так как H — подгруппа и $r = y - na$, то $r \in H$, а потому $r = 0$, и наше утверждение доказано.

Мы будем говорить, что группа G *циклическая*, если существует такой элемент a в G, что всякий элемент x из G может быть записан в виде a^n, где $n \in \mathbf{Z}$ (другими словами, если отображение $f: \mathbf{Z} \to G$, определяемое формулой $f(n) = a^n$, сюръективно). При этом элемент a называется *образующей* группы G.

Пусть G — группа и $a \in G$. Подмножество всех элементов a^n ($n \in \mathbf{Z}$) есть, очевидно, циклическая подгруппа в G. Если m — целое число, для которого $a^m = e$ и $m > 0$, то мы будем называть m *показателем* элемента a. Будем говорить, что $m > 0$ — *показатель* группы G, если $x^m = e$ для всех $x \in G$.

Пусть G — группа и $a \in G$. Пусть f: $\mathbf{Z} \to G$ — гомоморфизм, определенный формулой $f(n) = a^n$, и пусть H — ядро f. Возможны два случая.

(i) Ядро тривиально. Тогда f — изоморфизм $\mathbf{Z}$ на циклическую подгруппу в G, порожденную элементом a, и эта подгруппа бесконечна. (Если a порождает G, то G — циклическая группа.) Мы говорим, что a имеет *бесконечный период*.

(ii) Ядро не тривиально. Пусть d — наименьшее положительное целое число, лежащее в ядре. Это d называется *периодом* (или *порядком*) элемента a. Если m — такое целое число, что $a^m = e$, то $m = ds$ для некоторого целого s. Заметим, что элементы $e, a, \ldots, a^{d-1}$ попарно различны. Действительно, если $a^r = a^s$, где $0 \leqslant r, s \leqslant d - 1$, и, скажем, $r \leqslant s$, то $a^{s-r} = e$. Так как $0 \leqslant s - r < d$, то мы должны иметь $s - r = 0$. Циклическая подгруппа, порожденная элементом a, имеет порядок d. Следовательно, справедливо

Предложение 2. *Пусть G — конечная группа порядка $n > 1$. Тогда период всякого элемента $a \neq e$ из G делит n. Если порядок группы G — простое число p, то G — циклическая группа и любой отличный от e элемент служит образующей для G.*

Далее имеет место

Предложение 3. *Пусть G — циклическая группа. Тогда всякая ее подгруппа — циклическая. Если f — гомоморфизм G, то его образ — циклическая группа.*

Доказательство. Если G — бесконечная циклическая группа, то она изоморфна $\mathbf{Z}$, а мы нашли все подгруппы в $\mathbf{Z}$ и обнаружили, что они циклические. Если G — конечная циклическая группа с образующей a и H — некоторая ее подгруппа, то пусть m — наименьшее положительное целое число, такое, что a^m лежит в H. Легко проверяется, что a^m порождает H. Наконец, если f: $G \to G'$ — гомоморфизм и a — образующая для G, то $f(a)$ есть, очевидно, образующая для $f(G)$ и, следовательно, $f(G)$ — циклическая группа.

Мы предоставляем читателю в качестве упражнений доказательства следующих утверждений о циклических группах:

(i) *Бесконечная циклическая группа имеет в точности две образующие* (если a — образующая, то a^{-1} — единственная другая образующая).

(ii) Пусть G — конечная циклическая группа порядка n и x — ее образующая. *Множество образующих группы G состоит из тех степеней x^{ν} элемента x, в которых показатель ν взаимно прост с n.*

(iii) Пусть G — циклическая группа и a, b — две ее образующие. *Тогда существует автоморфизм группы G, переводящий a в b. Обратно, любой автоморфизм группы G переводит a в некоторую образующую G.*

§ 4. Нормальные подгруппы

Мы уже отмечали, что ядра гомоморфизмов групп являются подгруппами. Теперь мы хотим охарактеризовать такие подгруппы.

Пусть $f\colon G \to G'$ — гомоморфизм групп и H — его ядро. Для всякого элемента x из G выполняется равенство $xH = Hx$, что проверяется непосредственно исходя из определений. Мы можем также переписать это соотношение в виде $xHx^{-1} = H$.

Обратно, пусть G — группа и H — ее подгруппа. Предположим, что для всех элементов x из G имеем $xH \subset Hx$ (или, что эквивалентно, $xHx^{-1} \subset H$). Если мы возьмем x^{-1} вместо x, то получим $H \subset xHx^{-1}$, откуда $xHx^{-1} = H$. Таким образом, наше условие эквивалентно условию $xHx^{-1} = H$ для всех $x \in G$. Подгруппа H, удовлетворяющая этому условию, называется *нормальной* (или *инвариантной*) подгруппой. Мы сейчас увидим, что всякая нормальная подгруппа служит ядром некоторого гомоморфизма.

Пусть G' — множество смежных классов по H (по предположению левые смежные классы совпадают с правыми смежными классами, так что нет нужды делать различие между ними). Если xH и yH — смежные классы, то их произведение $(xH)(yH)$ также будет смежным классом, поскольку

$$xHyH = xyHH = xyH.$$

Это произведение определяет в G' ассоциативный закон композиции. Ясно, что сама подгруппа H как смежный класс служит единичным элементом для этого закона композиции и что $x^{-1}H$ служит обратным для смежного класса xH. Следовательно, G' — группа.

Пусть $f\colon G \to G'$ — отображение, для которого $f(x)$ есть смежный класс xH. Тогда, очевидно, f — гомоморфизм и подгруппа H содержится в его ядре. Если $f(x) = H$, то $xH = H$ и, значит, $x \in H$, так как H содержит единичный элемент. Таким образом, H совпадает с ядром, и мы получили интересовавший нас гомоморфизм.