МИНИСТЕРСТВО ВЫСШЕГО И СРЕДНЕГО СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ БССР

ГОМЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Л.А.Неметков

КЛАССИЧЕСКИЕ ФАКТОРИЗАЦИИ ГРУПП И КОЛЕЦ

(Учебное пособие)

Гомель 1979

УДК 519.4

Рецензенты: С.А.Чунихин, академик АН БССР, доктор физико-математических наук, профессор; А.П.Кохно, кандидат физико-математических наук, доцент

Учебное пособие посвящено изложению трех классических результатов алгебры: теоремы Жордана-Гёльдера о композиционных рядах групп, теоремы Ремака-Шмидта о прямых разложениях групп и теорем Молина-Веддерберна о строении полупростых и простых колец.

Предназначено для студентов старших курсов математических специальностей.

№ 20203 - 045 / М 339 - 79 6 - 79

ВВЕДЕНИЕ

Каждое целое число $m > 1$ представимо в виде произведения простых чисел, и если даны два разложения (факторизации) такого рода $m = p_1 p_2 \dots p_n = h_1 h_2 \dots h_\kappa$, то $n = \kappa$ и для некоторой перестановки $i \mapsto \alpha_i$ имеет место $p_i = h_{\alpha i}$, $i = 1, 2, \dots, \kappa$. Этот результат можно сформулировать иначе. Назовем цепочку

$$m = m_0 > m_1 > \dots > m_\kappa = 1$$

композиционным рядом числа m, если m_i делит m_{i-1} и m_{i-1}/m_i простое число, $i = 1, 2, \dots, \kappa$. Число κ назовем длиной, а m_{i-1}/m_i - фактором композиционного ряда числа m. В этих терминах теорема формулируется так: Целое число $m > 1$ имеет композиционный ряд, длины любых двух композиционных рядов числа m одинаковы, а между факторами этих двух рядов может быть установлено взаимно однозначное соответствие, при котором соответствующие факторы совпадают.

Сформулированная теорема имеет в алгебре многочисленные аналогии. Общей чертой многих исследований является стремление расчленить алгебраический объект на в каком-то смысле простые части, а затем доказать единственность полученных разложений (факторизаций). В 1870 году Жордан ввел понятие композиционного ряда конечной группы и доказал совпадение порядков факторов любых двух композиционных рядов конечной группы. В 1889 году Гёльдер дополнил теорему Жордана изоморфизмом соответствующих факторов. В дальнейшем теорема Жордана-Гёльдера получила развитие во многих направлениях. В 1934 году Цассенхауз доказал свою знаменитую лемму о бабочке, с помощью которой легко доказывается теорема Жордана-Гёльдера в самой общей формулировке (для необязательно конечных групп с произвольной областью операторов).

В качестве аналога простого числа можно рассматривать неразложимую группу, т.е. неединичную группу, не разложимую в прямое произведение двух неединичных подгрупп. В 1911 году Ремак доказал теорему об изоморфизме двух прямых разложений конечных групп с неразложимыми множителями. Этот результат в 1928 году был значительно улучшен О.Ю.Шмидтом, который рассматривал разложения необязательно конечных групп с произволь-

ной областью операторов. Теорему Шмидта обычно в литературе называют теоремой Ремака-Шмидта.

В конце XIX века проводились интенсивные исследования конечномерных ассоциативных алгебр над полем C комплексных чисел. Здесь выдающиеся результаты получил Ф.Э.Молин. В работе Ф.Э.Молина впервые ясно и отчетливо появляется радикал как наибольший нильпотентный идеал (сам термин "радикал" был введен Фробениусом в 1903 году). Ф.Э.Молин доказал, что факторалгебра по радикалу полупроста, полупростая алгебра разлагается в прямую сумму простых алгебр, а простые алгебры – это в точности алгебры матриц над C подходящих порядков. Этот замечательный результат получил развитие в работах Картана, а особенно в работах Веддербарна, который в 1908 году завершил построение структурной теории конечномерных ассоциативных алгебр над любым полем. В дальнейшем исследованиями Э.Нётер и Артина теория Молина-Веддербарна была распространена на ассоциативные кольца с условием минимальности для левых идеалов.

Настоящее пособие посвящено изложению трех отмеченных выше достижений алгебры: теоремы Жордана-Гёльдера, теоремы Ремака-Шмидта, а также теорем Молина-Веддербарна в общем виде, который был им придан усилиями многих математиков. В списке литературы приведены книги, к которым может обратиться заинтересованный читатель. С современным состоянием теории радикалов можно познакомиться по недавно вышедшей книге В.А.Андрунакиевича и Ю.М.Рябухина.

Необходимый для чтения минимум сведений из теории гр[illegible] помещен в дополнении. Начало и конец доказательства обозначается соответственно через Д и КД.

§ I. КОМПОЗИЦИОННЫЕ РЯДЫ ГРУПП

I. Эндоморфизмы. Эндоморфизмом группы G называется гомоморфизм группы G в G. Таким образом, эндоморфизм α группы G переводит элемент $x \in G$ в некоторый элемент $x^\alpha \in G$, причем $(xy)^\alpha = x^\alpha y^\alpha$ для любых $x, y \in G$. Эндоморфизм, являющийся изоморфизмом, называется автоморфизмом. Множество всех эндоморфизмов группы G обозначают через $End\,G$, а множество всех ее автоморфизмов – через $Aut\,G$.

Пример I.I. Отображение $x \mapsto e$ для любого $x \in G$ являет[ся], конечно, эндоморфизмом. Этот эндоморфизм называется нулевым. Автоморфизм $x \mapsto x$, $x \in G$, называют единичным (или тождественным).

Пример I.2. Если n – фиксированное целое число, G – абелева группа, то отображение $x \mapsto x^n$, $x \in G$, является эндоморфизмом. Эндоморфизм, получающийся таким способом, называется степенным. Можно показать, что все эндоморфизмы циклической группы являются степенными.

Пример I.3. Зафиксируем элемент $a \in G$ и рассмотрим отображение $\hat{a} : x \mapsto a^{-1}xa$, $x \in G$. Ввиду $a^{-1}Ga = G$ отображение $\hat{a}$ является перестановкой множества элементов G. Кроме того, $(xy)^{\hat{a}} = x^{\hat{a}} y^{\hat{a}}$. Поэтому $\hat{a}$ – автоморфизм G. Он называется внутренним автоморфизмом, индуцированным элементом a.

Автоморфизм группы G называют внутренним, если он совпадает с $\hat{a}$ для некоторого $a \in G$. Множество всех внутренних автоморфизмов группы G обозначают через $In\,G$.

Если $\alpha, \beta \in End\,G$, то произведение $\alpha\beta$, определяемое равенством $x^{(\alpha\beta)} = (x^\alpha)^\beta$, $x \in G$, также является эндоморфизмом G. Произведение автоморфизмов является автоморфизмом, и легко убедиться в том, что $Aut\,G$ с операцией умножения автоморфизмов является группой. Можно также показать, что $In\,G$ явл[яется] нормальной подгруппой группы $Aut\,G$, но этот факт нам не понадобится.

2. Операторы. Пусть дано множество Ω и отображение

$$f : \Omega \to End\,G, \qquad (1)$$

переводящее элемент α из Ω в элемент $f(\alpha)$ из $End\,G$. Тогда Ω называется областью операторов группы G, элементы из Ω – операторами, а сама группа G – Ω-группой или группой с областью операторов Ω. Операторы действуют на G так же, как и соответствующие им эндоморфизмы. Это означает, что $x^{\alpha}=x^{f(\alpha)}$ для любых $\alpha\in\Omega$, $x\in G$. Ясно, что для любых $\alpha\in\Omega$, $x,y\in G$ имеет место

$$x^{\alpha}\in G,\quad (xy)^{\alpha}=x^{\alpha}y^{\alpha}. \qquad (2)$$

Часто область операторов вводят заданием действия (2), что, конечно, автоматически определяет отображение (I). Заметим, что различные операторы могут не отличаться по действию, поскольку им может соответствовать один и тот же эндоморфизм.

Если M – часть группы G и $\alpha\in\Omega$, то M^{α} состоит из элементов вида x^{α}, где $x\in M$. Ясно, что если M – подгруппа, то и M^{α} – подгруппа.

Часть M группы G называется Ω-допустимой, если $M^{\alpha}\subseteq M$ для любого $\alpha\in\Omega$ (в этом случае говорят также, что M выдерживает операторы из Ω). Ω-допустимые подгруппы иначе называют Ω-подгруппами. Если M – Ω-подгруппа и $\alpha\in\Omega$, то ограничение $f(\alpha)$ на M принадлежит $End\,M$. Это позволяет считать Ω областью операторов любой Ω-подгруппы группы G.

Пример I.4. Пусть A – часть группы G. Превратим A в область операторов группы G, полагая $x^{a}=x^{\hat{a}}$, где $a\in A$, $x\in G$ (см.пример 1.3). Оператору $a\in A$ соответствует внутренний автоморфизм $\hat{a}\in In\,G$, причем $x^{a}=a^{-1}xa$ для всех $x\in G$. В частности, если $A=G$, то G-подгруппами группы G являются ее нормальные подгруппы и только они.

Пример I.5. Пусть V – левое линейное пространство над полем F. Тогда F является областью операторов аддитивной абелевой группы этого пространства (оператор $\alpha\in F$ переводит $v\in V$ в элемент αv), а всякая F-подгруппа является подпространством.

Теорема I.I. Пусть дано некоторое множество Ω-подгрупп $\{A_i\mid i\in I\}$ Ω-группы G. Тогда их пересечение $\bigcap_{i\in I}A_i$ также является Ω-подгруппой.

Доказательство осуществляется проверкой. Тот факт, что пересечение подгрупп есть подгруппа, вытекает и теоремы I.I

в случае $\Omega=\emptyset$. Ниже мы будем иметь в виду, что при $\Omega=\emptyset$ в формулировках и определениях знак Ω опускается (безоператорный случай). Заметим еще, что при $\Omega=G$ (пример I.4) из теоремы I.I вытекает, что пересечение нормальных подгрупп является нормальной подгруппой.

Если K – Ω-подгруппа группы G и $K\lhd G$, то фактор-группа G/K становится Ω-группой, если положить $(xK)^{\sigma}=x^{\sigma}K$ для $x\in G$, $\sigma\in\Omega$. Именно это имеют в виду, когда говорят о Ω-фактор-группах Ω-групп. Легко проверить справедливость следующей теоремы.

Теорема I.2. Пусть K – нормальная Ω-подгруппа Ω-группы G. Тогда справедливы утверждения:

I) каждая Ω-подгруппа из G/K имеет вид H/K, где H – некоторая Ω-подгруппа из G;

2) если H – Ω-подгруппа из G, содержащая K, то H/K – Ω-подгруппа группы G/K.

При $\Omega=G$ из теоремы I.2 вытекает, что $H/K\lhd G/K$ тогда и только тогда, когда $H\lhd G$, $H\supseteq K$.

.3. Теоремы о гомоморфизмах. Пусть даны группы G и Γ с одной и той же областью операторов Ω. Гомоморфизм $f:G\to\Gamma$ называется Ω-гомоморфизмом, если $(x^{f})^{\alpha}=(x^{\alpha})^{f}$ для любых $x\in G$, $\alpha\in\Omega$. Легко проверяется, что ядро

$$Ker\,f=\{x\in G\mid x^{f}=\varepsilon\text{ – единица группы }\Gamma\}$$

Ω-гомоморфизма f является нормальной Ω-подгруппой группы G, а образ $H^{f}=\{h^{f}\mid h\in H\}$ любой Ω-подгруппы H из G является Ω-подгруппой группы Γ. В частности, образ $Im\,f=G^{f}=\{x^{f}\mid x\in G\}$ Ω-гомоморфизма f является Ω-подгруппой группы Γ.

Ω-гомоморфизм $f:G\to\Gamma$ называется:

I) Ω-эпиморфизмом, если $Im\,f=\Gamma$;

2) Ω-мономорфизмом, если $Ker\,f=E$;

3) Ω-изоморфизмом, если f является одновременно Ω-эпиморфизмом и Ω-мономорфизмом (в этом случае говорят, что группы G и Γ Ω-изоморфны).

Линейные преобразования линейного пространства над полем K являются не чем иным, как K-эндоморфизмами аддитив-

ной абелевой группы этого пространства.

Теорема I.3. При любом Ω-гомоморфизме $f: G \to \Gamma$ группы $G/\mathrm{Ker} f$ и $\mathrm{Im} f$ Ω-изоморфны.

Д Проверка показывает, что отображение

$$\varphi: x\,\mathrm{Ker} f \mapsto x^f, \quad x \in G,$$

является изоморфизмом группы $G/\mathrm{Ker} f$ на группу $\mathrm{Im} f$ (см. [1], теорема I § 3 гл.7). Если $\alpha \in \Omega$, то $((x\,\mathrm{Ker} f)^\alpha)^\varphi = (x^\alpha \mathrm{Ker} f)^\varphi = (x^\alpha)^f = (x^f)^\alpha = ((x\,\mathrm{Ker} f)^\varphi)^\alpha$. КД

Обратим внимание на то, что если $f: G \to \Gamma$ есть Ω-мономорфизм, то $f: G \to \mathrm{Im} f$ есть Ω-изоморфизм.

Теорема I.4. Пусть H, K - нормальные Ω-подгруппы Ω-группы G, причем $H \supseteq K$. Тогда H/K - нормальная Ω-подгруппа группы G/K и имеет место Ω-изоморфизм

$$(G/K)/(H/K) \cong G/H.$$

Д То, что H/K - нормальная Ω-подгруппа в G/K, вытекает из теоремы I.2. Таким образом, мы имеем возможность построить Ω-фактор-группы G/H и $(G/K)/(H/K)$. Рассмотрим отображение $f: xK \mapsto xH$, $x \in G$. Если $xK = yK$, то $y = xk$, $k \in K \subseteq H$ и $f: yK \mapsto yH = xkH = xH$. Значит, определение f не зависит от выбора представителя смежного класса. Теперь проверяем, что $f: G/K \to G/H$ есть Ω-эпиморфизм с ядром $\mathrm{Ker} f = H/K$. Остается применить теорему I.3. КД

Часто в выражении $(G/K)/(H/K)$ скобки опускают и пишут $G/K/H/K$.

Лемма I.I. Пусть B и H - такие Ω-подгруппы Ω-группы G, что $BH = HB$. Тогда BH является Ω-подгруппой.

Д Если $b \in B$, $h \in H$, $\alpha \in \Omega$, то $(bh)^\alpha = b^\alpha h^\alpha \in BH$, так как $b^\alpha \in B$, $h^\alpha \in H$. Это означает, что множество BH является Ω-допустимым. Покажем, что BH - подгруппа. Для этого достаточно показать, что $(bh)(b_1h_1)^{-1} \in BH$, где $b, b_1 \in B$, $h, h_1 \in H$. Ввиду $HB = BH$ элемент $hh_1^{-1}b_1^{-1}$ совпадает с b_2h_2 для некоторых $b_2 \in B$, $h_2 \in H$. Итак, $(bh)(b_1h_1)^{-1} = bhh_1^{-1}b_1^{-1} = (bb_2)h_2$, $bb_2 \in B$, $h_2 \in H$. КД

Из леммы I.I вытекает, что произведение двух перестановочных подгрупп является подгруппой (случай $\Omega = \emptyset$). Заметим, что две подгруппы перестановочны, если одна из них нормальна во всей группе. Следствием леммы I.I является и тот факт, что произведение двух нормальных подгрупп группы G является нормальной подгруппой в G (случай $\Omega = G$).

Теорема I.5. Пусть B, H - Ω-подгруппы Ω-группы G, причем $H \lhd G$. Тогда BH и $B \cap H$ являются Ω-подгруппами, $B \cap H \lhd B$, а Ω-фактор-группы BH/H и $B/B \cap H$ Ω-изоморфны.

Д По теореме I.I, $B \cap H$ является Ω-подгруппой. Рассматривая B как область операторов для групп B и H (действие сопряжением, как в примере I.4), мы видим, что подгруппа $B \cap H$ является B-допустимой, т.е. $B \cap H \lhd B$.

Так как $H \lhd G$, то $BH = HB$. Значит, по лемме I.I произведение BH является Ω-подгруппой. Нетрудно проверить, что отображение $f: b \mapsto bH$, где $b \in B$, является гомоморфизмом B в BH/H, причем $\mathrm{Ker} f = B \cap H$, $\mathrm{Im} f = BH/H$. Если $b \in B$, $\alpha \in \Omega$, то $(bf)^\alpha = b^\alpha H = (b^\alpha)f$, т.е. f - Ω-эпиморфизм. Остается применить теорему I.3. КД

4. Лемма Цассенхауза. Докажем сначала одно простое, но часто используемое утверждение.

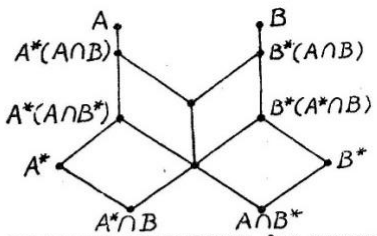
Лемма I.2. Пусть A, B, C - такие подгруппы группы G, что $AB = BA$ и $A \subseteq C$. Тогда $A(B \cap C) = AB \cap C$.

Д Если $a \in A$, $d \in B \cap C$, то из $A \subseteq C$ получаем $a \in C$, $ad \in C$. Из $a \in A$, $d \in B$ вытекает $ad \in AB$. Значит, $A(B \cap C) \subseteq AB \cap C$.

Если $x \in AB \cap C$, то $x \in AB$, $x \in C$. Значит, $x = ab$ для некоторых $a \in A$, $b \in B$. Так как $A \subseteq C$ и $x \in C$, то $b = a^{-1}x \in C$. Значит, $x = ab \in A(B \cap C)$. Таким образом, $AB \cap C \subseteq A(B \cap C)$. КД

Заметим, что из теоремы I.I и леммы I.I следует, что в условии леммы I.2 пересечение $AB \cap C$ является подгруппой.

Следующая лемма принадлежит Цассенхаузу. Ее часто называют леммой о бабочке, поскольку фигурирующие в ней подгруппы расположены следующим образом.



Здесь точками изображены подгруппы. Одна подгруппа содержится в другой, если она соединена с ней линией, идущей вверх.

Лемма I.3 (Лемма Цассенхауза). Пусть даны Ω-подгруппы A, A^*, B, B^* Ω-группы G, причем $A^* \lhd A$, $B^* \lhd B$. Тогда $A^*(A\cap B)$, $A^*(A\cap B^*)$, $B^*(A\cap B)$, $B^*(A^*\cap B)$ являются Ω-подгруппами, причем $A^*(A\cap B^*) \lhd A^*(A\cap B)$, $B^*(A^*\cap B) \lhd B^*(A\cap B)$ и имеет место Ω-изоморфизм

$$A^*(A\cap B)/A^*(A\cap B^*) \simeq B^*(A\cap B)/B^*(A^*\cap B).$$

Д Вспомним, что по теореме I.I пересечение Ω-подгрупп является Ω-подгруппой. Так как $A^* \lhd A$ и $A\cap B \subseteq A$, то по теореме I.5 пересечение $A^*\cap(A\cap B) = A^*\cap B$ является нормальной Ω-подгруппой в Ω-подгруппе $A\cap B$. Аналогично, $A\cap B^* \lhd A\cap B$. По лемме I.I, $(A^*\cap B)(A\cap B^*)$ является нормальной Ω-подгруппой в $A\cap B$.

Так как $A^* \lhd A$, то $A^*(A\cap B^*) = (A\cap B^*)A^*$ и по лемме I.I $A^*(A\cap B^*)$ является Ω-подгруппой. Произведение $A^*(A\cap B)$ также является Ω-подгруппой. Всякая группа допустима относительно любой своей части (действие сопряжением). Поэтому $A^*(A\cap B^*)$ является A^*-допустимой. Так как $A^* \lhd A$, то A^* является $(A\cap B)$-допустимой. Так как $A\cap B^* \lhd A\cap B$, то мы видим, что $A^*(A\cap B^*)$ является $(A\cap B)$-допустимой и A^*-допустимой (при действии сопряжением). Таким образом, $A^*(A\cap B^*)$ является нормальной Ω-подгруппой Ω-подгруппы $A^*(A\cap B)$.

Применим теперь теорему I.5 к Ω-группе $A^*(A\cap B)$, ее Ω-подгруппе $A\cap B$ и нормальной Ω-подгруппе $A^*(A\cap B^*)$.

Имеем Ω-изоморфизм:

$$A^*(A\cap B)/A^*(A\cap B^*) = (A\cap B)(A^*(A\cap B^*))/A^*(A\cap B^*) \simeq$$
$$\simeq (A\cap B)/(A\cap B)\cap(A^*(A\cap B^*))$$

Подгруппы A^* и $A\cap B^*$ перестановочны, причем $A\cap B^* \subseteq A\cap B$. По лемме I.2, $(A\cap B^*)(A^*\cap B) = (A\cap B^*)((A^*\cap(A\cap B)) =$ $= A^*(A\cap B^*)\cap(A\cap B)$. Учитывая это, имеем Ω-изоморфизм:

$$A^*(A\cap B)/A^*(A\cap B^*) \simeq (A\cap B)/(A^*\cap B)(A\cap B^*) \quad (1)$$

Точно так же устанавливается, что $B^*(A^*\cap B)$ является нормальной Ω-подгруппой в Ω-подгруппе $B^*(A\cap B)$ и существует Ω-изоморфизм

$$B^*(A\cap B)/B^*(A^*\cap B) \simeq (A\cap B)/(A^*\cap B)(A\cap B^*) \quad (2)$$

Остается сравнить (1) и (2). КД

5. Ряды подгрупп. Ω-рядом Ω-группы G называется конечная последовательность Ω-подгрупп вида

$$G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_t = E, \quad t \geqslant 0. \qquad (*)$$

Число t называется длиной Ω-ряда $(*)$. Ω-ряд $(*)$ называется:

1) нормальным Ω-рядом, если $G_i \lhd G$ для любого $i = 1,2,\dots,t$;

2) субнормальным Ω-рядом, если $G_i \lhd G_{i-1}$ для любого $i = 1,2,\dots,t$.

Если Ω-ряд $(*)$ субнормален, то можно составить Ω-фактор-группы G_{i-1}/G_i, $1 \leq i \leq t$, которые называются факторами ряда $(*)$.

Ряд $(*)$ можно уплотнить, вставляя Ω-подгруппы между соседними членами G_{i-1} и G_i. Полученный ряд называется уплотнением ряда $(*)$.

Весьма важно понятие Ω-изоморфизма Ω-рядов. Два субнормальных Ω-ряда называют Ω-изоморфными, если длины их одинаковы и существует взаимно однозначное отображение множества всех факторов одного ряда на множество всех факторов другого ряда, при котором соответствующие факторы Ω-изоморфны.

Теорема I.6 (Шрейер). Любые два субнормальных Ω-ряда Ω-группы G можно так уплотнить, что получатся Ω-изоморфные субнормальные Ω-ряды.

Д Пусть даны два субнормальных Ω-ряда Ω-группы G :

$$G = H_0 \supseteq H_1 \supseteq \dots \supseteq H_s = E, \qquad (1)$$

$$G = K_0 \supseteq K_1 \supseteq \dots \supseteq K_t = E. \qquad (2)$$

При $S=1$ утверждение очевидно. Поэтому пусть $S>1, t>1$. Введем следующие обозначения: $H_{i,j} = H_i(H_{i-1} \cap K_j)$, $K_{i,j} = K_j(K_{j-1} \cap H_i)$. Применим лемму I.3, положив в ней $A=H_{i-1}, B=H_i, A^*=H_i, B^*=K_j$. Мы получим тогда, что $H_{i,j}$ есть нормальная Ω-подгруппа Ω-подгруппы $H_{i,j-1}$, а $K_{i,j}$ есть нормальная Ω-подгруппа Ω-подгруппы $K_{i-1,j}$, причем группы $H_{i,j-1}/H_{i,j}$ и $K_{i-1,j}/K_{i,j}$ Ω-изоморфны. Подгруппами $H_{i,j}$ и $K_{i,j}$ $(1 \le i \le s,\ 1 \le j \le t)$ мы уплотним ряды (I) и (2), получая

$$\dots \supseteq H_{i,0} \supseteq H_{i,1} \supseteq \dots \supseteq H_{i,j-1} \supseteq H_{i,j} \supseteq \dots \supseteq H_{i,t} \supseteq \dots \quad (3)$$

$$\dots \supseteq K_{0,j} \supseteq K_{1,j} \supseteq \dots \supseteq K_{i-1,j} \supseteq K_{i,j} \supseteq \dots \supseteq K_{s,j} \supseteq \dots \quad (4)$$

Заметим, что $H_{i,0} = H_{i-1}$, $H_{i,t} = H_i$, $K_{0,j} = K_{j-1}$, $K_{s,j} = K_j$. Ряды (3) и (4), как следует из построения, субнормальны и являются уплотнениями рядов (I) и (2). Длины рядов (3) и (4) равны st, а их факторы $H_{i,j-1}/H_{i,j}$ и $K_{i-1,j}/K_{i,j}$ Ω-изоморфны. КД

При $\Omega = \varnothing$ из теоремы I.6 получаем

Следствие I.6.I. Любые два субнормальных ряда группы G обладают уплотнениями, являющимися изоморфными субнормальными рядами.

6. Теорема Жордана-Гёльдера. Мы подошли к одному из трех главных результатов этой книги. В теореме Жордана-Гёльдера речь идет об Ω-изоморфизме субнормальных Ω-рядов специального вида.

Ω-группа G называется Ω-простой, если $G \neq E$ и в G нет нормальных Ω-подгрупп, отличных от G и E. Ω-простая подгруппа - это Ω-подгруппа, являющаяся Ω-простой группой.

Ряд без повторений $G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_t = E$ Ω-группы

$G \neq E$ назовем:

I) Ω-композиционным рядом, если он является субнормальным Ω-рядом и группа G_{i-1}/G_i Ω-проста для любого $i = 1,2,\dots,t$.

2) Ω-главным рядом, если он является нормальным Ω-рядом и между G_{i-1} и G_i нельзя вставить ни одной Ω-подгруппы, нормальной в G и отличной от G_{i-1} и G_i, $i = 1,2,\dots,t$.

Факторы Ω-композиционных (Ω-главных) рядов группы G называют Ω-композиционными (соответственно Ω-главными) факторами группы G.

Ряд $E \supseteq E$ будем считать Ω-композиционным и Ω-главным для единичной группы E. Число 0 будем считать длиной Ω-композиционного и Ω-главного ряда группы $G = E$.

Теорема I.7 (Жордан-Гёльдер). Любые два Ω-композиционных ряда Ω-группы G Ω-изоморфны. Любые два Ω-главных ряда Ω-группы G Ω-изоморфны.

Д Если $G = E$, то утверждение верно. Пусть $G \neq E$. По теореме I.6, Ω-композиционные ряды (R_1) и (R_2) группы G обладают Ω-изоморфными уплотнениями (R_1^*) и (R_2^*). Из Ω-простоты фактора G_{i-1}/G_i следует, что если $G_{i-1} \supseteq H \supseteq G_i$ и H - нормальная Ω^i-подгруппа в G_{i-1}, то либо $H = G_{i-1}$, либо $H = G_i$. Поэтому множество всех неединичных факторов ряда (R_1^*) совпадает с множеством всех факторов ряда (R_1), а множество всех неединичных факторов ряда (R_2^*) совпадает с множеством всех факторов ряда (R_2). Теперь видно, что из Ω-изоморфизма рядов (R_1^*) и (R_2^*) следует Ω-изоморфизм рядов (R_1) и (R_2). Первое утверждение теоремы доказано.

Второе утверждение теоремы является частным случаем первого, поскольку Ω-ряд является Ω-главным тогда и только тогда, когда он является $(\Omega \cup \Pi_G)$-композиционным. КД

Знак Ω опускается при $\Omega = \varnothing$, и мы получаем определение композиционного и главного ряда, а также

Следствие I.7.I. Любые два композиционных ряда группы G изоморфны. Любые два главных ряда группы G изоморфны.

В теореме I.7 ничего не говорилось о существовании рядов. Пример бесконечной циклической группы (см. [1], теорема 6 § 3 гл.4) показывает, что группа может и не обладать композиционными рядами. Понятно, что конечные Ω-группы имеют Ω-композиционные и Ω-главные ряды. Займемся нахождением

условия существования таких рядов у произвольной Ω-группы.

Подгруппа H Ω-группы G называется Ω-субнормальной, если H является членом некоторого субнормального Ω-ряда группы G.

Лемма I.4. Пусть H - Ω-субнормальная подгруппа Ω-группы G. Тогда H является Ω-субнормальной подгруппой в любой ее содержащей Ω-подгруппе группы G.

Д Пусть $H \subseteq B$, где B - Ω-подгруппа. По условию существует цепь Ω-подгрупп

$$G = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_k = H$$

такая, что $H_i \lhd H_{i-1}$ для любого $i = 1, 2, \ldots, k$. Пусть $B_i = H_i \cap B$; $i = 0, 1, \ldots, k$. Подгруппы B_i являются Ω-подгруппами по теореме I.1. Так как $B_{i-1} \cap H_i = B_i$, $H_i \lhd H_{i-1}$ и $B_{i-1} \subseteq H_{i-1}$, то по теореме I.5 $B_i \lhd B_{i-1}$. Значит, цепь $B = B_0 \supseteq B_1 \supseteq \ldots \supseteq B_k = H$ состоит из Ω-подгрупп, каждая из которых нормальна в предыдущей. Значит, H Ω-субнормальна в G. ∎

Говорят, что Ω-группа G удовлетворяет условию минимальности для Ω-субнормальных подгрупп, если всякая убывающая цепь ее Ω-субнормальных подгрупп $G \supset \ldots$ конечна (т.е. обрывается на конечном члене). Ω-группа G такова, что всякая возрастающая цепь Ω-субнормальных подгрупп $H_1 \subset H_2 \subset \ldots$ конечна, назовем ее, удовлетворяет условию максимальности для Ω-субнормальных подгрупп.

Теорема I.8. Ω-группа G тогда и только тогда обладает хотя бы одним Ω-композиционным рядом, когда G удовлетворяет условиям минимальности и максимальности для Ω-субнормальных подгрупп.

Д Пусть $G \neq E$ обладает Ω-композиционным рядом

$$G = G_0 \supset G_1 \supset \ldots \supset G_t = E. \qquad (I)$$

Предположим, что G имеет ряд подгрупп

$$G = K_0 \supset K_1 \supset \ldots \supset K_n = E \qquad (2)$$

такой, что $n > t$ и K_i Ω-субнормальна в G для любого

$i = 1, 2, \ldots, n$. По лемме I.4 для любого $i \geq 1$ подгруппа K_i Ω-субнормальна в K_{i-1}. Поэтому ряд (2) можно уплотнить и получить субнормальный Ω-ряд (3) длины $\geq n$, не имеющий повторений. По теореме I.6, существуют Ω-изоморфные субнормальные Ω-ряды (4) и (5), являющиеся уплотнениями соответственно рядов (I) и (3). Ряд (4) имеет t неединичных факторов, а ряд (5) имеет не менее n неединичных факторов, причем $n > t$. Получили противоречие. Мы доказали, что каждый ряд без повторений, составленный из Ω-субнормальных подгрупп, имеет длину, не превышающую t. Отсюда сразу следует, что G удовлетворяет условиям минимальности и максимальности для Ω-субнормальных подгрупп. Необходимость доказана.

Достаточность. Пусть $G \neq E$ удовлетворяет условиям минимальности и максимальности для Ω-субнормальных подгрупп. Из того, что все возрастающие цепи Ω-субнормальных подгрупп конечны, следует существование убывающей цепи

$$G = M_0 \supset M_1 \supset \ldots$$

такой, что для любого $i \geq 1$ подгруппа M_i является Ω-субнормальной подгруппой в G, причем между M_{i-1} и M_i нельзя вставить ни одной подгруппы, Ω-субнормальной в G и отличной от M_{i-1} и M_i. Из леммы I.4 следует, что $M_i \lhd M_{i-1}$, а ввиду условия минимальности для Ω-субнормальных подгрупп $M_t = E$ для некоторого t. Мы получаем искомый Ω-композиционный ряд $G = M_0 \supset M_1 \supset \ldots \supset M_t = E$. ∎

Примером группы, удовлетворяющей условию теоремы I.8, может служить аддитивная абелева группа V конечномерного линейного пространства над бесконечным полем F. Поле F выступает здесь как область операторов для V.

Если рассматривать цепи нормальных Ω-подгрупп, то мы приходим к условию минимальности (максимальности) для нормальных Ω-подгрупп. Фактически здесь нет нового понятия, так как условие минимальности (максимальности) для нормальных Ω-подгрупп совпадает с условием минимальности (максимальности) для $(\Omega \cup In G)$-субнормальных подгрупп. Поэтому из теоремы I.8 вытекает

Следствие I.8.I. Ω-группа G тогда и только тогда обладает хотя бы одним Ω-главным рядом, когда G удовлетворяет условиям минимальности и максимальности для нормальных Ω-подгрупп.

§ 2. ПРЯМЫЕ РАЗЛОЖЕНИЯ ГРУПП

I. Прямые произведения. Пусть дано некоторое непустое множество нормальных подгрупп $\{H_\kappa \mid \kappa \in I\}$ группы G. Обозначим через $\Pi_{\kappa\in I} H_\kappa$ множество всех тех элементов группы G, которые представимы в виде произведения конечного числа элементов некоторых из подгрупп H_κ, $\kappa \in I$. Множество $\Pi_{\kappa\in I} H_\kappa$ называется произведением нормальных подгрупп H_κ, $\kappa \in I$, и само является, как легко проверить, нормальной подгруппой в G. Среди произведений нормальных подгрупп выделяются прямые произведения.

Говорят, что группа G разлагается в прямое произведение своих подгрупп A_i, $i \in I$, и пишут $G = \times_{i\in I} A_i$, если выполняются следующие условия:

1) $A_i \lhd G$ для любого $i \in I$;

2) $G = \Pi_{i\in I} A_i$;

3) при $|I| > 1$ для любого $j \in I$ имеет место $A_j \cap \Pi_{i\neq j} A_i = 1$.

Подгруппы A_i называются множителями данного прямого произведения, которое иначе называется прямым разложением группы G. Если $I = \{1, 2, \dots, n\}$, то применяется также запись

$$G = \times_{i=1}^{n} A_i = A_1 \times A_2 \times \dots \times A_n .$$

Лемма 2.1. Если $G = \times_{i\in I} A_i$, то при любых $\kappa \neq \ell$ каждый элемент из A_κ перестановочен с каждым элементом из A_ℓ.

Д Очевидно, $A_\kappa A_\ell = A_\kappa \times A_\ell$. Пусть $a \in A_\kappa$, $b \in A_\ell$. Рассмотрим элемент $a^{-1}b^{-1}ab$. Так как $A_\kappa \lhd G$, то $b^{-1}ab \in A_\kappa$, а значит, $a^{-1}(b^{-1}ab) \in A_\kappa$. Так как $A_\ell \lhd G$, то $(a^{-1}b^{-1}a)b \in A_\ell$. Таким образом, $a^{-1}b^{-1}ab \in A_\kappa \cap A_\ell = E$, т.е. $a^{-1}b^{-1}ab = e$, $ab = ba$. КД

Лемма 2.2. Пусть $A_1, A_2, \dots, A_t$ – нормальные подгруппы группы G. Тогда следующие условия эквивалентны:

1) $G = A_1 \times A_2 \times \dots \times A_t$;

2) каждый элемент $x \in G$ единственным образом представим в виде $x = a_1 a_2 \dots a_t$, где $a_i \in A_i$, $i = 1, 2, \dots, t$.

Замечание. Элемент a_i называется A_i-компонентой элемента x в данном прямом произведении.

Д Пусть дано 1), $x = a_1 a_2 \dots a_t = a_1' a_2' \dots a_t'$, где $a_i, a_i' \in A_i$. Тогда

$$(a_1')^{-1} a_1 = (a_2' \dots a_t')(a_2 \dots a_t)^{-1} \in A_1 \cap (A_2 \dots A_t) = E,$$

откуда $a_1 = a_1'$.

Пусть дано 2), $x \in A_j \cap \Pi_{i\neq j} A_i$. Тогда $x = a_1 \dots a_{j-1} e a_{j+1} \dots a_t$, где $a_i \in A_i$. Это равенство показывает, что A_j-компонента элемента x равна e. Но ввиду $x \in A_j$ элемент $x = e \dots e x e \dots e$ совпадает со своей A_j-компонентой. Значит, $x = e$. КД

Лемма 2.3. Если

$$G = (A_1 \times A_2 \times \dots \times A_t) \times (A_{t+1} \times A_{t+2} \times \dots \times A_n),$$

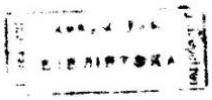
то $G = A_1 \times A_2 \times \dots \times A_n$.

Д Из леммы 2.1 выводим, что все A_i нормальны в G. Ясно, что $G = \Pi_{i=1}^{n} A_i$. Пусть элемент $x \in G$ двумя способами представим в виде $x = a_1 a_2 \dots a_n = a_1' a_2' \dots a_n'$, где $a_i, a_i' \in A_i$. Из леммы 2.2 вытекает, что $a_1 a_2 \dots a_t = a_1' a_2' \dots a_t'$, $a_{t+1} a_{t+2} \dots a_n = a_{t+1}' a_{t+2}' \dots a_n'$. Снова применяя лемму 2.2, теперь уже к произведениям $A_1 \times A_2 \times \dots \times A_t$ и $A_{t+1} A_{t+2} \dots A_n$, получаем $a_i = a_i'$ для любого i. КД

Лемма 2.4. Пусть Ω-группа G представима в виде прямого произведения своих Ω-подгрупп: $G = A_1 \times A_2 \times \dots \times A_t$. Построим отображение $\varphi_i : x \mapsto a_i$, где a_i – A_i-компонента элемента $x \in G$. Тогда отображение $\varphi_i : G \to A_i$ является Ω-эндоморфизмом группы G и если H – Ω-подгруппа из G, то H^{φ_i} – Ω-подгруппа из A_i.

Замечание. Эндоморфизм φ_i назовем проектированием G в A_i, а подгруппу H^{φ_i} – проекцией подгруппы H в A_i. В частности, G^{φ_i} – проекция группы G в A_i.

Д Существование отображения φ_i обусловлено леммой 2.2 (единственность A_i-компоненты). Из этой же леммы вытекает так же, что A_i-компонента элемента xy равна произведению A_i-компонент элементов $x, y \in G$. Значит, φ_i – гомоморфизм G в A_i. Поскольку для любого $a \in A_i$ имеем $\varphi_i : a \mapsto a$, то $A^{\varphi_i} = A_i$. Пусть $x \in \Omega$, $x = a_1 a_2 \dots a_t$, где



$a_1 \in A_1, a_2 \in A_2, \dots, a_t \in A_t$. Тогда $x^\alpha = a_1^\alpha a_2^\alpha \dots a_t^\alpha$, и так как A_i - Ω-подгруппа, то a_i^α принадлежит A_i и является A_i-компонентой элемента x^α. Это означает, что $(x^\alpha)\varphi_i = (x\varphi_i)^\alpha = a_i^\alpha$, т.е. φ_i - Ω-гомоморфизм. КД

Лемма 2.5. Если $G = A \times B$ и H - подгруппа, содержащая A, то $H = A \times (H \cap B)$.

Д Так как $A \subseteq H$ и $AB = BA = G$, то по лемме I.2 имеем $A(H \cap B) = H \cap AB = H \cap G = H$. По теореме I.5, $H \cap B \lhd H$. Так как $A \cap (H \cap B) = A \cap B = E$, то $H = A \times (H \cap B)$. КД

2. Центр и G-автоморфизмы. Определим нормализатор $N_G(M)$ части M группы G как множество всех $x \in G$, для которых $Mx = xM$.

Лемма 2.6. $N_G(M)$ является подгруппой для любой части M группы G.

Д Пусть $x, y \in N_G(M)$. Из $yM = My$ следует $My^{-1} = y^{-1}M$, поэтому $y^{-1} \in N_G(M)$, а значит, $xy^{-1} \in N_G(M)$. КД

Если $N_G(M) = G$, то часть M называется нормальной в G. В соответствии с терминологией п.2 § I часть M нормальна в G тогда и только тогда, когда M выдерживает все внутренние автоморфизмы группы G (заметим, что условие $Mx = xM$ равносильно $M^x = x^{-1}Mx = M$).

Множество $Z(G)$ всех нормальных элементов группы G содержит e и является, очевидно, нормальной подгруппой группы G.

Лемма 2.7. Если $G = A_1 \times A_2 \times \dots \times A_t$, $t > 1$, и H - часть подгруппы A_1, то

$$N_G(H) = N_{A_1}(H) \times A_2 \times \dots \times A_t,$$
$$Z(G) = Z(A_1) \times Z(A_2) \times \dots \times Z(A_t).$$

Д Пусть $B = A_2 \times A_3 \times \dots \times A_t$. По лемме 2.1, $B \subseteq N_G(H)$. Кроме того, $N_G(H) \cap A_1 = N_{A_1}(H)$. Поэтому, ввиду леммы 2.5, получаем $N_G(H) = N_{A_1}(H) \times B$.

Пусть $K = \prod_{i=1}^{t} Z(A_i)$. По доказанному $Z(A_i) \lhd G$ для

любого i. Поэтому достаточно установить, что $K = Z(G)$.

Если $a \in Z(A_i)$, то по доказанному $N_G(a) = G$. Это означает, что $K \subseteq Z(G)$. Представим элемент $z \in Z(G)$ в виде $z = a_1 a_2 \dots a_t$, где $a_i \in A_i$. Если y - произвольный элемент из A_1, то

$$zy = yz = (a_1 y)a_2 \dots a_t = (ya_1)a_2 \dots a_t.$$

Согласно лемме 2.2, $a_1 y = ya_1$, т.е. $a_1 \in Z(A_1)$. Аналогично, $a_i \in Z(A_i)$ для любого i, т.е. $z \in K$. Итак, $K = Z(G)$. КД

Будем рассматривать $Inn G$-автоморфизмы группы G, т.е. те автоморфизмы, которые перестановочны с каждым внутренним автоморфизмом группы G. Выше мы условились считать группу G областью операторов для самой себя (пример I.4). Поэтому G-автоморфизм и $Inn G$-автоморфизм - это одно и то же. Часто G-автоморфизмы группы G называют центральным автоморфизмом. Это название оправдывается следующей леммой.

Лемма 2.8. Пусть $\alpha \in Aut\, G$. Тогда следующие условия эквивалентны:

1) α - центральный автоморфизм группы G;

2) $x(x^\alpha)^{-1} \in Z(G)$ для любого $x \in G$.

Д Пусть α - G-автоморфизм. Тогда для любых $x, y \in G$ имеем:

$$(x^\alpha)^{-1}(y^\alpha)x^\alpha = (x^{-1}yx)^\alpha = (yx)^\alpha = (y^\alpha)x = x^{-1}y^\alpha x,$$

откуда $x(x^\alpha)^{-1}y^\alpha = y^\alpha x(x^\alpha)^{-1}$. Значит, $x(x^\alpha)^{-1}$ перестановочен с любым элементом вида y^α, где $y \in G$. Так как α - автоморфизм, то $\{y^\alpha \mid y \in G\} = G$. Значит, утверждение 2) верно.

Пусть теперь дано 2). Тогда для любых $x, y \in G$ имеем $(x(x^\alpha)^{-1})y^\alpha = y^\alpha(x(x^\alpha)^{-1})$, откуда

$$(x^\alpha)^{-1}y^\alpha x^\alpha = x^{-1}y^\alpha x = (y^\alpha)^x.$$

Так как левая часть этого равенства равна $(x^{-1}yx)^\alpha$, то мы и получаем, что α - G-автоморфизм. КД

Лемма 2.9. Если $Z(G) = E$, то G не имеет неединичных центральных автоморфизмов.

Д Если α - G-автоморфизм, то по лемме 2.8 для любого

$x \in G$ имеем $x(x^{\alpha})^{-1} = e$, откуда $x = x^{\alpha}$. КД

Лемма 2.10. Пусть Ω-группа G двумя способами представима в виде прямого произведения Ω-подгрупп: $G = A \times B_1 = A \times B_2$. Тогда G обладает центральным Ω-автоморфизмом переводящим B_1 в B_2.

Д Отображение $\varphi_i : b_i \mapsto b_i A$, где $b_i \in B_i$, является Ω-изоморфизмом B_i на G/A, $i = 1,2$. Поэтому $\varphi = \varphi_1 \varphi_2^{-1}$ является Ω-изоморфизмом B_1 на B_2. Если $b \in B_1$, то по построению $Ab = Ab^{\varphi}$, откуда $b = ab^{\varphi}$, $a \in A$. Если y - любой элемент из A, то $b_1(y)$ содержит по лемме 2.1 подгруппы B_1 и B_2, а значит, содержит и элемент $b(b^{\varphi})^{-1} = a$. Это означает, что a перестановочен с каждым элементом из A, т.е. $a \in Z(A) \subseteq Z(G)$. Итак, доказано, что

$$b(b^{\varphi})^{-1} \in Z(G) \text{ для любого } b \in B_1. \quad (*)$$

Так как каждый элемент $x \in G$ единственным образом представим в виде $x = ab_1$, где $a \in A$, $b_1 \in B_1$, то мы можем построить отображение $f : x \mapsto ab_1^{\varphi}$, сужение которого на B_1 совпадает с φ. Ввиду леммы 2.1, без труда проверяется, что f - эндоморфизм группы G. Если $\sigma \in \Omega$, то

$$(x^f)^{\sigma} = a^{\sigma} b_1^{\varphi\sigma} = a^{\sigma} b_1^{\sigma\varphi} = ((ab_1^{\varphi})^{\sigma})^f = (x^{\sigma})^f,$$

т.е. f - Ω-эндоморфизм. Ясно также, что A и B_1 входят в G^f, причем $\mathrm{Ker}\, f = E$, т.е. f - автоморфизм. Учитывая (*), получаем:

$$x(x^f)^{-1} = ab_1(ab_1^{\varphi})^{-1} = ab_1(b_1^{\varphi})^{-1}a^{-1} = b_1(b_1^{\varphi})^{-1} \in Z(G).$$

По лемме 2.8, f - центральный автоморфизм. КД

3. Теорема Ремака-Шмидта. Введем следующее определение. Ω-подгруппа A Ω-группы G называется Ω-неразложимой, если A отлична от E и не может быть представлена в виде прямого произведения двух неединичных Ω-подгрупп. При $A = G$ мы получаем понятие Ω-неразложимой группы.

Ω-подгруппа $A \neq E$ называется Ω-разложимой, если она не является Ω-неразложимой.

При $\Omega = \emptyset$ мы приходим к понятию неразложимой и разложимой подгруппы (в частности, группы).

Теорема 2.1. Пусть G - неединичная Ω-группа, обладающая Ω-главным рядом. Тогда G представима в виде прямого произведения конечного числа своих Ω-неразложимых Ω-подгрупп.

Д Будем доказывать теорему индукцией по длине Ω-главного ряда группы. Если G Ω-неразложима, то теорема верна, и искомое прямое произведение в этом случае содержит лишь один множитель.

Пусть G Ω-разложима. Это значит, что G представима в виде $G = G_1 \times G_2$, где G_1 и G_2 - неединичные Ω-подгруппы. Из леммы 2.7 следует, что каждая нормальная подгруппа из G_i нормальна в G. Следовательно, согласно следствию I.8.1, G_1 и G_2 удовлетворяют условиям минимальности и максимальности для нормальных Ω-подгрупп и обладают Ω-главными рядами. Понятно, что длины Ω-главных рядов групп G_1 и G_2 меньше длины Ω-главного ряда G. Поэтому по индукции G_1 и G_2 представимы в виде прямого произведения Ω-неразложимых Ω-подгрупп:

$$G_1 = A_1 \times A_2 \times \ldots \times A_t, \quad G_2 = A_{t+1} \times A_{t+2} \times \ldots \times A_n.$$

Ввиду леммы 2.3, отсюда и из $G = G_1 \times G_2$ получаем искомое разложение $G = A_1 \times A_2 \times \ldots \times A_n$. КД

Мы убедились в том, что доказательство существования прямых разложений с Ω-неразложимыми множителями не представляет особого труда. Гораздо более трудной является проблема изоморфизма таких разложений. Эта проблема для конечных групп была решена Ремаком, а в общем случае (для операторных групп с главными рядами) - О.Ю.Шмидтом. Прежде чем приступить к формулировке и доказательству знаменитой теоремы Ремака-Шмидта, приведем одну простую лемму, которая нам понадобится.

Лемма 2.11. Пусть Ω-группа G представима в виде $G = G_1 G_2$, где G_1 и G_2 - нормальные Ω-подгруппы группы G. Если l, l_1, l_2, l_3 - длины Ω-композиционных рядов соответственно групп $G, G_1, G_2, G_1 \cap G_2$, то $l = l_1 + l_2 - l_3$.

Д Очевидно, $G/G_1 \cap G_2 = (G_1/G_1 \cap G_2) \times (G_2/G_1 \cap G_2)$. Длины Ω-композиционных рядов групп $G/G_1 \cap G_2$, $G_1/G_1 \cap G_2$ и $G_2/G_1 \cap G_2$ соответственно равны $l - l_3$, $l_1 - l_3$ и $l_2 - l_3$. Поэтому лемму достаточно доказать только для случая $G_1 \cap G_2 = E$. Пусть $G_1 \cap G_2 = E$, $G_1 \neq E$, $G_2 \neq E$ и

$$G_1 = H_0 \supset H_1 \supset \ldots \supset H_{l_1} = E, \quad G_2 = M_0 \supset M_1 \supset \ldots \supset M_{l_2} = E$$

являются Ω-композиционными рядами групп G_1 и G_2. Из $G_1 \cap G_2 = E$ и леммы I.2 получаем $M_{i-1} \cap G_1 \; M_i = M_i (M_{i-1} \cap G_1) = M_i$. Поэтому $G_1 M_{i-1} / G_1 M_i$ и M_{i-1}/M_i Ω-изоморфны, и ряд

$$G = M_0 G_1 \supset M_1 G_1 \supset \ldots \supset M_{\ell_2} G_1 \supset H_1 \supset H_2 \supset \ldots \supset H_{\ell_1} = E$$

является Ω-композиционным рядом группы G. Значит, $\ell = \ell_1 + \ell_2$. КД

Теорема 2.2 (Ремак-Шмидт). Пусть неединичная Ω-группа двумя способами представлена в виде прямого произведения своих Ω-неразложимых Ω-подгрупп:

$$G = H_1 \times H_2 \times \ldots \times H_\kappa , \qquad (I)$$

$$G = F_1 \times F_2 \times \ldots \times F_s . \qquad (2)$$

Тогда справедливы следующие утверждения:

I) Для любого множителя H_i разложения (I) найдется такой множитель F_{κ_i} разложения (2), что

$$G = F_{\kappa_i} \times (X_{j \neq i} H_j) = H_i \times (X_{j \neq \kappa_i} F_j) ;$$

2) $\kappa = s$ и отображение $i \to \kappa_i$ является перестановкой чисел $1, 2, \ldots, \kappa$;

3) для каждого $i = 1, 2, \ldots, \kappa$ существует центральный Ω-автоморфизм φ_i группы G такой, что $H_i^{\varphi_i} = F_{\kappa_i}$.

Замечание. При $\kappa = 1$ мы считаем, что

$$X_{j \neq i} H_j = X_{j \neq \kappa_i} F_j = E .$$

Д Расширим область операторов Ω, полагая $\Lambda = \Omega \cup In\, G$. Тогда Λ-подгруппами будут лишь нормальные Ω-подгруппы, Λ-композиционный ряд - это Ω-главный ряд. Ясно, что если мы докажем теорему для G с областью операторов Λ, то тем самым теорема будет доказана и для G с областью операторов Ω. Поэтому сразу будем считать, что Ω содержит все внутренние автоморфизмы группы G. Заметим, что тогда Ω-автоморфизмы группы G будут центральными.

Ради удобства и только в данном доказательстве мы через $\ell(G)$ будем обозначать длину Ω-композиционного (или, что то же самое в нашем случае, Ω-главного) ряда группы G. Если

$\ell(G) = 1$, то $\kappa = s = 1$, и теорема верна. Пусть $\ell(G) > 1$ и предположим по индукции, что теорема верна для всех неединичных Ω-групп R с $\ell(R) < \ell(G)$. Мы будем доказывать сначала утверждение I), которое словами выражают так: H_i и F_{κ_i} замещают друг друга в разложениях (I) и (2). В конце доказательства мы увидим, что из I) легко следуют утверждения 2) и 3).

Доказательство утверждения I) проведем для множителя H_1 и установим, что H_1 и некоторый множитель разложения (2) замещают друг друга. Обозначим через F_{i1} проекцию H_1 в множитель F_i разложения (2). По лемме 2.4, F_{i1} является Ω-подгруппой. Рассмотрим два случая.

СЛУЧАЙ 1: $F_{i1} \neq F_i$ для некоторого i, $1 \leq i \leq s$.

Каждый элемент из H_1 представим в виде произведения элементов из $F_{11}, F_{21}, \ldots, F_{s1}$. Поэтому H_1 содержится в Ω-подгруппе $\bar{G} = \Pi_{j=1}^{s} F_{j1} = X_{j=1}^{s} F_{j1}$. Так как $F_{i1} \subset F_i$, то $\ell(F_{i1}) < \ell(F_i)$. По лемме 2.II, $\ell(G) = \sum_{j=1}^{s} \ell(F_j)$, $\ell(\bar{G}) = \sum_{j=1}^{s} \ell(F_{j1})$. Мы видим, что $\ell(\bar{G}) < \ell(G)$, значит, теорема для $\bar{G}$ верна. Применяя теорему 2.I и лемму 2.3 к подгруппам F_{j1}, $1 \leq j \leq s$, мы получаем прямое разложение

$$\bar{G} = L_1 \times L_2 \times \ldots \times L_n \qquad (3)$$

с Ω-неразложимыми множителями, принадлежащими подгруппам F_{j1}. По лемме 2.5,

$$\bar{G} = H_1 \times D, \qquad (4)$$

где $D = \bar{G} \cap \Pi_{j=2}^{\kappa} H_j$ является Ω-подгруппой как пересечение Ω-подгрупп. Если $D \neq E$, то разложение (4) можно продолжить до прямого разложения с Ω-неразложимыми множителями, применяя к D теорему 2.I. Так как для $\bar{G}$ теорема верна, то можно утверждать, что H_1 и некоторый множитель разложения (3), пусть H_1 и L_1, Ω-изоморфны и замещают друг друга в (3) и (4):

$$\bar{G} = H_1 \times L_2 \times \ldots \times L_n = L_1 \times D, \; L_1 \subseteq F_{m1}, \; 1 \leq m \leq s .$$

Так как $L_1 \cap D = E$, то

$$L_1 \cap \Pi_{j=2}^{K} H_j = L_1 \cap \bar{G} \cap \Pi_{j=2}^{K} H_j = L_1 \cap D = E.$$

Поэтому $L_1 \Pi_{j=2}^{K} H_j = L_1 \times H_2 \times \ldots \times H_K$. Эта подгруппа, ввиду Ω-изоморфизма $L_1 \simeq H_1$ и леммы 2.II, имеет Ω-композиционный ряд длины $\ell(G)$. Поэтому $G = L_1 \times H_2 \times \ldots \times H_K$. Так как $L_1 \subseteq F_{m1} \subseteq F_m$, то по лемме 2.5 имеем $F_m = L_1 \times (F_m \cap (H_2 \times \ldots \times H_K))$. Отсюда и из Ω-неразложимости подгруппы F_m следует, что $F_{m1} = F_m = L_1$. Таким образом, получается, что

$$G = F_m \times (X_{j=2}^{K} H_j), \quad F_{m1} = F_m \simeq H_1. \qquad (5)$$

Каждый элемент $h \in H_1$ представим в виде $h = f_1 f_2 \ldots f_s$, где $f_j \in F_{j1} \subseteq F_j$. Отсюда следует, что $f_m = h \Pi_{j \neq m} f_j^{-1}$ принадлежит $H_1 \Pi_{j \neq m} F_j$. Так как $F_{m1} = F_m$, то $F_m \subseteq H_1 \Pi_{j \neq m} F_j$. Мы приходим к равенству:

$$G = H_1 \Pi_{j \neq m} F_j. \qquad (6)$$

По лемме 2.II, из (2) и (6) получаем:

$$\ell(G) = \ell(F_m) + \ell(\Pi_{j \neq m} F_j) = \ell(H_1) + \ell(\Pi_{j \neq m} F_j) - \ell(H_1 \cap \Pi_{j \neq m} F_j).$$

Так как ввиду Ω-изоморфизма $F_m \simeq H_1$ имеет место равенство $\ell(F_m) = \ell(H_1)$, то должно быть $\ell(H_1 \cap \Pi_{j \neq m} F_j) = 0$. Мы приходим, таким образом, к прямому произведению:

$$G = H_1 \times (X_{j \neq m} F_j). \qquad (7)$$

Равенства (5) и (7) показывают, что H_1 и F_m замещают друг друга в разложениях (1) и (2), причем $F_{m1} = F_m$.

СЛУЧАЙ 2: $F_{i1} = F_i$ для любого $i = 1, 2, \ldots, s$.

Рассмотрим два подслучая случая 2.

СЛУЧАЙ 2.1: для некоторого i проекция F_i в множитель H_1 разложения (I) совпадает с H_1.

Пусть, для определенности, проекция F_1 в H_1 совпадает с H_1. Тогда $H_1 \subseteq F_1 \Pi_{j=2}^{K} H_j$ (этот факт устанавливается тем же простым рассуждением, которое применялось выше при установлении равенства (6)). Ввиду равенства (I), мы получаем

$$G = F_1 (X_{j=2}^{K} H_j). \qquad (8)$$

В рассматриваемом случае проекция F_{11} подгруппы H_1 в F_1 совпадает с F_1. Поэтому $F_1 \subseteq H_1 \Pi_{j=2}^{S} F_j$, и мы приходим к равенству

$$G = H_1 (X_{j=2}^{S} F_j). \qquad (9)$$

Применяя лемму 2.II к (8) и (I), получаем:

$$\ell(G) = \ell(X_{j=2}^{K} H_j) + \ell(F_1) - \ell(F_1 \cap (X_{j=2}^{K} H_j)),$$

$$\ell(G) = \ell(X_{j=2}^{K} H_j) + \ell(H_1).$$

Значит, $\ell(F_1) \geqslant \ell(H_1)$. Аналогично, применяя лемму 2.II к (9) и (2), получаем $\ell(H_1) \geqslant \ell(F_1)$. Итак, $\ell(H_1) = \ell(F_1)$. Но тогда

$$\ell(F_1 \cap (X_{j=2}^{K} H_j)) = \ell(H_1 \cap (X_{j=2}^{S} F_s)) = 0,$$

а это означает, что произведения (8) и (9) – прямые, т.е.

$$G = F_1 \times H_2 \times \ldots \times H_K = H_1 \times F_2 \times \ldots \times F_s.$$

СЛУЧАЙ 2.2: для любого $i = 1, 2, \ldots, s$ проекция H_{i1} подгруппы F_i в множитель H_1 разложения (I) не совпадает с H_1.

Мы имеем возможность применить рассмотренный случай I к каждой из подгрупп $F_1, F_2, \ldots, F_s$. Обозначим через H_{ij} проекцию F_i в множитель H_j разложения (I). По доказанному, F_1 и некоторая подгруппа H_{K_1}, такая, что $H_{1K_1} = H_{K_1}$, замещают друг друга в (I) и (2), т.е.

$$G = H_{K_1} \times (X_{j=2}^{S} F_s). \qquad (10)$$

Рассматриваем разложения (I0) и (I). Так как проекция F_2 в H_1 не совпадает с H_1, то по доказанному (случай I) F_2 и

некоторая подгруппа H_{K_2} со свойством $H_2 K_2 = H_{K_2}$ занимают друг друга в разложениях (I) и (I0), т.е.

$$G = H_{K_1} \times H_{K_2} \times \left(\bigtimes_{j=3}^{S} F_S\right). \qquad (II)$$

Так как проекция F_3 в H_1 не совпадает с H_1, то мы применяем рассмотренный случай I к подгруппе F_3 и разложениям (II) и (I). Продолжая этот процесс, мы на S-том шаге придем к равенству

$$G = H_{K_1} \times H_{K_2} \times \ldots \times H_{K_S}, \qquad (I2)$$

множители которого удовлетворяют условию: $H_{iK_i} = H_{K_i}$. Сравнение (I2) и (I) показывает, что $K = S$, а значит, для некоторого i имеет место $K_i = 1$. Получили противоречие, так как в рассматриваемом случае $H_{i1} \neq H_1$ для любого i. Значит, случай 2.2 невозможен. Следовательно, утверждение I) теоремы полностью доказано.

ОКОНЧАНИЕ ДОКАЗАТЕЛЬСТВА. Согласно доказанному утверждению I), найдется такая подгруппа F_{K_1}, что H_1 и F_{K_1} занимают друг друга в разложениях (I) и (2), а значит

$$G = F_{K_1} \times H_2 \times \ldots \times H_K. \qquad (I3)$$

Из леммы 2.I0, примененной к (I) и (I3), получаем, что группа G обладает Ω-автоморфизмом φ_1, переводящим H_1 в F_{K_1}.

Применим теперь утверждение I) к (2) и (I3). Тогда

$$G = F_{K_1} \times F_{K_2} \times H_3 \times \ldots \times H_K \qquad (I4)$$

для некоторой подгруппы F_{K_2} такой, что $H_2^{\varphi_2} = F_{K_2}$, где φ_2 - Ω-автоморфизм группы G, существующий по лемме 2.I0. Применяем затем утверждение I) к (2) и (I4). Продолжая процесс, мы на K-том шаге придем к равенству

$$G = F_{K_1} \times F_{K_2} \times \ldots \times F_{K_K} \qquad (I5)$$

к существованию Ω-автоморфизма φ_i группы G, переводящего H_i в F_{K_i}, $i = 1, 2, \ldots, K$. Сравнение (I5) и (2) показывает, что $K = S$ и отображение $i \mapsto K_i$ является перестановкой.

Если G конечна и $\Omega = \varnothing$, то из теоремы 2.2 получается

Теорема 2.3 (Remak). Пусть конечная группа G двумя способами разложена в прямое произведение неразложимых подгрупп:

$$G = H_1 \times H_2 \times \ldots \times H_K = F_1 \times F_2 \times \ldots \times F_S.$$

Тогда $K = S$ и при подходящей нумерации существует нормальный автоморфизм φ_i группы G такой, что $H_i^{\varphi_i} = F_i$, $i = 1, \ldots, K$.

4. Вполне приводимые группы. Если для каждой нормальной Ω-подгруппы A Ω-группы G найдется такая нормальная Ω-подгруппа B, что $G = A \times B$, то G называется вполне приводимой Ω-группой.

Лемма 2.I2. Пусть G - вполне приводимая Ω-группа. Тогда:

1) каждая нормальная Ω-подгруппа нормальной Ω-подгруппы группы G нормальна в G;

2) каждая нормальная Ω-подгруппа группы G является вполне приводимой Ω-группой.

▲ Пусть G - вполне приводимая Ω-группа, K - ее нормальная Ω-подгруппа. Тогда K выделяется в G при некотором множителем, т.е. $G = K \times M$, где M - Ω-подгруппа. Если H - нормальная Ω-подгруппа из K, то по лемме 2.7 $H \lhd G$. По условию, $G = H \times R$, где R - Ω-подгруппа. По лемме 2.5, $K = H \times (K \cap R)$, т.е. K вполне приводима. ▼

Теорема 2.4. Следующие три утверждения относительно неединичной Ω-группы G эквивалентны:

1) Ω-группа G вполне приводима;

2) G разлагается в прямое произведение Ω-простых подгрупп;

3) G разлагается в произведение (необязательно прямое) нормальных Ω-простых подгрупп.

▲ Пусть дано I). Рассмотрим нормальную Ω-подгруппу $M \neq E$ группы G и докажем, что M обладает Ω-простой нормальной подгруппой. Зафиксируем неединичный элемент $a \in M$ и рассмотрим множество $\mathfrak{M}$ всех тех нормальных Ω-подгрупп из M, которые не содержат элемент a. Очевидно, $E \in \mathfrak{M}$. Пусть некоторое множество $\{R_i \in \mathfrak{M} \mid i \in I\}$ образует цепь, т.е. $R_i \subseteq R_j$, либо $R_j \subseteq R_i$ для любых $i, j \in I$. Тогда объединение $\bigcup_{i \in I} R_i$ этой цепи, как легко видеть, принадлежит $\mathfrak{M}$. Следовательно, по лемме Цорна (см. [6], с.60) $\mathfrak{M}$ имеет максимальный элемент N. По лемме 2.I2, $M = N \times N_1$, где N_1 - нормальная Ω-подгруппа из G. Так как $N \neq M$,

то $N_1 \neq E$.Предположим, что N_1 содержит нетривиальную нормальную Ω-подгруппу N_2 . Тогда по лемме 2.I2 имеем $N_1 = N_2 \times N_3$, где N_3 - нормальная Ω-подгруппа. Рассмотрим произведение $M = N \times N_2 \times N_3$. Если $a \in NN_2 \cap NN_3$, то $a = nn_2 = n_1 n_3$, где $n, n_1 \in N$, $n_2 \in N_2$, $n_3 \in N_3$. Применяя лемму 2.2, получаем $n_2 = n_3 = e$. Значит, $NN_2 \cap NN_3 = N$. Так как $a \notin N$, то отсюда вытекает, что либо $a \notin NN_2$, либо $a \notin NN_3$. Но это противоречит максимальности N в $\mathfrak{M}$. Остается предположить , что подгруппа N Ω-проста.

Мы доказали, что каждая неединичная нормальная Ω-подгруппа (в частности, сама G) имеет нормальную Ω-простую подгруппу. Пусть $\{S_i \mid i \in I\}$ - множество всех нормальных Ω-простых подгрупп группы G . Обозначим через Λ множество всех таких подмножеств J множества I , что $\prod_{j \in J} S_j = \times_{j \in J} S_j$. Легко видеть, что объединение всякой цепи элементов множества Λ снова принадлежит Λ .Значит, по принципу максимума в Λ имеется максимальный элемент Λ_0 . Предположим, что $G^* = \times_{i \in \Lambda_0} S_i \neq G$. В силу полной приводимости группа G имеет такую нормальную Ω-подгруппу G^{**}, что $G = G^* \times G^{**}$. По доказанному G^{**} имеет нормальную Ω-простую подгруппу S_κ, $\kappa \in J$. Значит, $G^* S_\kappa = \times_{i \in \Lambda_1} S_i$, где $\Lambda_1 = \Lambda \cup \{\kappa\}$. Но это противоречит максимальности Λ_0. Итак, доказано, что из I) следует 2).

Очевидно, из 2) следует 3). Пусть дано 3). Докажем, что тогда верно I). Пусть M - произвольная нормальная Ω-подгруппа группы G. По принципу максимума существует максимальная (по включению $\subseteq$) нормальная Ω-подгруппа M^* такая, что $MM^* = M \times M^*$. Допустим, что $M \times M^* \neq G$. Пусть x - элемент из G , не входящий в $M \times M^*$. По условию, $x = x_1 x_2 \dots x_t$, где x_i принадлежит нормальной Ω-простой подгруппе S_{κ_i}, $i = 1,2,\dots,t$. Так как $x \notin MM^*$, то $x_j \notin MM^*$ для некоторого j , а значит, S_{κ_j} не входит в MM^*. Так как S_{κ_j} Ω-проста, то отсюда получаем $MM^* \cap S_{\kappa_j} = E$, и мы приходим к прямому произведению $MM^* S_{\kappa_j} = M \times M^* \times S_{\kappa_j}$. Отсюда следует, что $M^* \subset M^* \times S_{\kappa_j}$ и $(M^* \times S_{\kappa_j}) \cap M = E$. Но это противоречит максимальности M^*. Остается принять, что $M \times M^* = G$. КД

Следствие 2.4.I. Пусть G - вполне приводимая Ω-группа. Тогда следующие утверждения эквивалентны:

I) G удовлетворяет условию максимальности для нормальных Ω-подгрупп;

2) G удовлетворяет условию минимальности для нормальных Ω-подгрупп.

△ По теореме 2.4, $G = \times_{i \in I} S_i$, где S_i Ω-просты. Тогда возрастающей последовательности $I_1 \subset I_2 \subset \dots$ подмножеств множества I соответствует возрастающая цепь нормальных Ω-подгрупп

$$\times_{i \in I_1} S_i \subset \times_{i \in I_2} S_i \subset \dots , \qquad (1)$$

а убывающей последовательности $I \supset J_1 \supset J_2 \supset \dots$ соответствует убывающая цепь

$$G \supset \times_{i \in J_1} S_i \supset \times_{i \in J} S_i \supset \dots \qquad (2)$$

Пусть дано I). Тогда цепь (I) конечна, т.е.

$$G = \times_{i \in I_k} S_i \qquad (3)$$

для некоторого k . Более того, из I) следует, что множество I_k конечно, пусть $I_k = \{1,2,\dots,t\}$. Ряд $E \subset S_1 \subset S_1 S_2 \subset \dots \subset S_1 S_2 \dots S_i \subset \dots \subset G$ является Ω-главным рядом, поскольку его факторы изоморфны группам S_i и, значит, Ω-просты. По следствию I.8.I, G удовлетворяет условию минимальности для нормальных Ω-подгрупп.

Если верно 2), то цепь (2) конечна, и с учетом следствия I.8.I мы получаем I). КД

Следствие 2.4.2. Неединичная Ω-группа G , обладающая Ω-главным рядом, вполне приводима тогда и только тогда, когда G разлагается в прямое произведение конечного числа Ω-простых подгрупп.

§ 3. РАЗЛОЖЕНИЯ В КОЛЬЦАХ

I. Кольца. В этом пункте мы напомним начальные сведения о кольцах. Непустое множество R с двумя бинарными алгебраическими операциями $+$ и $\cdot$, называемыми сложением и умножением, называется кольцом, если выполняются следующие условия:

1) R с операцией $+$ является абелевой группой; эта группа называется аддитивной группой кольца и обозначается через $(R,+)$;

2) $a(bc)=(ab)c$ для любых $a,b,c\in R$;

3) $(a+b)c=ac+bc$, $c(a+b)=ca+cb$ для всех $a,b,c\in R$.

Кольцо обозначается через $(R,+,\cdot)$, но чаще всего говорят, что R является кольцом, понимая при этом, что множество R надо рассматривать вместе с операциями $+$ и $\cdot$.

Из того, что $(R,+)$ - группа, следует, что кольцо R имеет нулевой элемент 0, для которого $0+a=a+0=a$ для всех $a\in R$. То, что нулевой элемент кольца и число нуль обозначаются одинаково, не приводит к недоразумениям, поскольку всегда ясно, о каком нуле идет речь. Для любого $a\in R$ имеется противоположный элемент $-a$, причем $a+(-a)=0$. Если в R имеется такой элемент e, что $ea=ae=a$ для любого $a\in R$, то e называется единицей кольца R. Кольцо R называется коммутативным, если $ab=ba$ для всех $a,b\in R$.

Разность $a-b$ элементов a и b определяется равенством $a-b=a+(-b)$. Из определения кольца без труда выводится справедливость следующих равенств:

$$0\cdot a=a\cdot 0=0,\quad (-a)b=a(-b)=-ab,\quad (-a)(-b)=ab,$$

$$-(a_1+a_2+\ldots+a_n)=-a_1-a_2-\ldots-a_n.$$

Поскольку умножение и сложение в кольце ассоциативно, то в длинных произведениях и суммах скобки можно опускать. Если m - положительное целое число, то полагают $a^m=aa\ldots a$ (m сомножителей), $ma=am=a+a+\ldots+a$ (m слагаемых), $(-m)a=a(-m)=-(ma)$. Полагают также, что нулевой элемент кольца совпадает с $0a=a0$, где $0\in\mathbb{Z}$, $a\in R$. Нетрудно установить справедливость следующих равенств:

$$(a_1+a_2+\ldots+a_k)(b_1+b_2+\ldots+b_m)=\sum_{i=1}^{k}\sum_{j=1}^{m}a_ib_j,$$

$$n(ab)=a(nb)=(na)b,$$

$$(n_1+n_2)a=n_1a+n_2a,$$

где $a_i,b_i,a,b\in R$, $n,n_1,n_2\in\mathbb{Z}$.

Непустое подмножество K кольца R называется подкольцом, если K является подгруппой аддитивной группы кольца R и $ab\in K$ для любых $a,b\in K$ (говорят также, что множество K замкнуто относительно умножения). Ясно, что подкольцо является кольцом относительно операций $+$ и $\cdot$. Нулевое подкольцо $0=(0)$ - это подкольцо, состоящее только из одного нулевого элемента 0. Нетрудно заметить, что непустое подмножество K кольца R тогда и только тогда является подкольцом, когда $ab\in K$, $a-b\in K$ для любых $a,b\in K$. Простой проверкой устанавливается, что пересечение любого семейства подколец кольца R является подкольцом.

Пусть R и R^* - кольца. Отображение $f: R\to R^*$ называется гомоморфизмом кольца R в кольцо R^*, если для любых $a,b\in R$ имеет место $(ab)^f=a^fb^f$, $(a+b)^f=a^f+b^f$. Гомоморфизм f называется:

1) эпиморфизмом, если его образ $\mathrm{Im}f=R^f=\{r^f\mid r\in R\}$ совпадает с R^*;

2) мономорфизмом, если его ядро $\mathrm{Ker}f=\{r\in R\mid r^f=0^*\}$ - нуль кольца R^f - совпадает с (0);

3) изоморфизмом, если $R^f=R^*$, $\mathrm{Ker}f=(0)$ (в этом случае говорят, что кольца R и R^* изоморфны и пишут $R\cong R^*$).

Заметим, что если $f: R\to R^*$ есть мономорфизм, то $f: R\to R^f$ есть изоморфизм. Эпиморфизм иначе называют гомоморфизмом на R^*.

2. Кольцо эндоморфизмов абелевой группы. Пусть дана аддитивная абелева группа A. Слово "аддитивная" означает, что групповая операция в данном случае обозначается знаком $+$ (сложение), а вместо единицы и обратного элемента мы говорим о нуле 0 и противоположном элементе $-a$. Рассмотрим $\mathrm{End}\,A$ - для аддитивных групп образ элемента x при гомоморфизме χ удобнее обозначать через $x\chi$, что мы и будем де-

лать в дальнейшем. Произведение эндоморфизмов определяется, как мы знаем, равенством $x(\alpha\beta)=(x\alpha)\beta$, где $x\in A$, $\alpha,\beta\in End\,A$. Введем операцию сложения эндоморфизмов. Если $\alpha,\beta\in End\,A$, то сумму $\alpha+\beta$ определяем равенством $x(\alpha+\beta)=x\alpha+x\beta$, где $x\in A$; из коммутативности группы A следует, что $\alpha+\beta\in End\,A$.

Множество $End\,A$, где A - аддитивная абелева группа, с введенными операциями сложения и умножения является кольцом. Тождественный автоморфизм ε группы A является единицей кольца $End\,A$.

Теорема 3.1. Любое кольцо изоморфно подкольцу кольца эндоморфизмов некоторой абелевой группы.

Д Пусть дано кольцо R. Предположим, что R не имеет единицы, и рассмотрим $R^*=\{(a,k)\,|\,a\in R, k\in\mathbb{Z}\}$. Введем операции сложения и умножения элементов из R^*: $(a,k)(b,n)=(ab+na+kb,kn)$, $(a,k)+(b,n)=(a+b,k+n)$. Тогда R^* с введенными операциями является кольцом с единицей $(0,1)$. Отображение $a\mapsto(a,0)$ является мономорфизмом R в R^*. Мы доказали, что любое кольцо изоморфно вкладывается в кольцо с единицей. Поэтому в дальнейшем будем считать, что R обладает единицей $e\neq 0$. Каждому $\tau\in R$ поставим в соответствие отображение $\hat{\tau}: R\to R$, определяемое равенством $x\hat{\tau}=x\tau$, где $x\in R$. Ясно, что $\hat{\tau}$ является эндоморфизмом аддитивной группы $A=(R,+)$ кольца R. Если предположить, что для некоторых элементов $\tau_1\neq\tau_2$ имеет место $\hat{\tau}_1=\hat{\tau}_2$, то мы сразу получаем противоречие, так как из $e\tau_1=e\tau_2$ следует $\tau_1=\tau_2$. Так как $\widehat{\tau_1\tau_2}=\hat{\tau}_1\hat{\tau}_2$, то мы получаем, что отображение $\tau\mapsto\hat{\tau}$ является мономорфизмом кольца R в $End\,A$. КД

3. Модули. Пусть дана аддитивная абелева группа A с областью операторов R, являющейся кольцом, причем для любых $x\in A$, $\tau_1,\tau_2\in R$ выполняются равенства

$$x(\tau_1\tau_2)=(x\tau_1)\tau_2,\quad x(\tau_1+\tau_2)=x\tau_1+x\tau_2. \qquad (1)$$

Тогда A называется правым R-модулем. Если кольцо R обладает единицей e, то дополнительно требуется, чтобы $xe=x$ для любого $x\in A$.

Равенства (1) показывают, что отображение, переводящее оператор $\tau\in R$ в соответствующий ему элемент из $End\,A$, является гомоморфизмом кольца R в кольцо $End\,A$.

Понятие левого R-модуля вводится аналогично, только умножение оператора на элемент группы производят слева. Таким образом, аддитивная абелева группа A с кольцом операторов R называется левым R-модулем, если:

1) образ элемента $x\in A$ под действием оператора $\tau\in R$ записывается в виде τx;

2) $(\tau_1\tau_2)x=\tau_1(\tau_2x)$, $(\tau_1+\tau_2)x=\tau_1x+\tau_2x$ для любых $\tau_1,\tau_2\in R$, $x\in A$. Если R обладает единицей e, то дополнительно требуется выполнение равенства $ex=x$ для любого $x\in A$.

Заметим, что в случае левого R-модуля A отображение f, переводящее оператор $\tau\in R$ в соответствующий ему элемент $f(\tau)\in End\,A$, будет антигомоморфизмом [7], поскольку $f(\tau_1+\tau_2)=f(\tau_1)+f(\tau_2)$, $f(\tau_1\tau_2)=f(\tau_2)f(\tau_1)$ для всех $\tau_1,\tau_2\in R$.

Пусть дан R-модуль A (правый, либо левый). Тогда R-подгруппы группы A называются R-подмодулями или просто подмодулями. Подмодуль H R-модуля A называется разложимым, неразложимым, вполне приводимым, если он является соответственно R-разложимой, R-неразложимой, вполне приводимой R-подгруппой. Неприводимый подмодуль - это R-простая R-подгруппа группы A. Понятно также, что означает термин R-модуль с условием минимальности или максимальности для подмодулей. Следует иметь в виду, что поскольку группа A аддитивна, то вместо прямых произведений следует говорить о прямых суммах. Так, разложимый подмодуль R-модуля A представим в виде прямой суммы ненулевых подмодулей. Гомоморфизм правого (левого) R-модуля A в правый (левый) R-модуль B определять нет необходимости, поскольку это не что иное, как R-гомоморфизм R-группы A в R-группу B.

Примерами левых и правых модулей являются левые и правые векторные пространства над полями. Для нас особое значение имеют следующие два примера.

Пример 3.1. Для фиксированного элемента α кольца R отображение $x\mapsto x\alpha$, $x\in R$, является эндоморфизмом аддитивной группы кольца R. Этот эндоморфизм называется правым умножением. Сопоставляя каждому элементу кольца R производи-

мое им правое умножение, мы превращаем аддитивную группу кольца R в правый R-модуль. Полученный таким образом модуль обозначают через R_R и называют правым регулярным модулем.

Пример 3.2. Левый регулярный модуль ${}_RR$ – это левый R-модуль, аддитивная группа которого совпадает с аддитивной группой кольца R, а операторы действуют как левые умножения, т.е. произведение оператора $r \in R$ на элемент модуля ${}_RR$ определяется как произведение rx в кольце R.

4. Идеалы. Левым (правым) идеалом кольца R называется всякий подмодуль модуля ${}_RR$ (соответственно модуля R_R). Двусторонним идеалом кольца R называется такая подгруппа аддитивной группы кольца R, которая одновременно является и левым и правым идеалом. Слово "двусторонний" часто опускают и говорят об идеалах, имея в виду двусторонние идеалы. Понятно, что в коммутативном кольце левые и правые идеалы являются двусторонними. Следующая лемма является перефразировкой введенных определений.

Лемма 3.1. Непустое множество I кольца R является:

1) левым идеалом, если $a-b \in I, ra \in I$ для всех $a, b \in I$, $r \in R$;

2) правым идеалом, если $a-b \in I, ar \in I$ для всех $a, b \in I$, $r \in R$.

В любом кольце R идеалами являются само кольцо R и нулевое подкольцо (0). Эти идеалы называют тривиальными.

Пусть A и B – непустые подмножества множества элементов кольца R. Их суммой будем называть множество $A+B=\{a+b \mid a \in A, b \in B\}$. Под произведением множеств A и B будем понимать множество AB, состоящее из всех конечных сумм вида $a_1b_1+\ldots+a_kb_k$, где $a_i \in A, b_i \in B$. Естественно вводится сумма и произведение нескольких множеств. Степень A^n, $n>0$, определяется как произведение $AA\ldots A$ (n множителей).

Лемма 3.2. Если $a \in R$ и M – подгруппа аддитивной группы кольца R, то

$$Ma=\{ma \mid m \in M\},\ aM=\{am \mid m \in M\}.$$

Доказательство очевидно.

Мы будем использовать также следующее обозначение:

$$a\mathbb{Z}=\mathbb{Z}a=\{na \mid n \in \mathbb{Z}\},$$ где a – элемент кольца R; очевидно, $a\mathbb{Z}$ является подгруппой аддитивной группы кольца R.

Лемма 3.3. Сумма любых двух левых, правых или двусторонних идеалов кольца R является соответственно левым, правым или двусторонним идеалом кольца R.

Д Пусть A и B – левые идеалы кольца R, x и y – любые элементы из $A+B$. Тогда $x=a_1+b_1$, $y=a_2+b_2$, где $a_1, a_2 \in A$, $b_1, b_2 \in B$. Если $r \in R$, то $rx=ra_1+rb_1 \in A+B$, поскольку $ra_1 \in A$, $rb_1 \in B$. Кроме того, $x-y=(a_1-a_2)+(b_1-b_2)$, где $(a_1-a_2) \in A$, $(b_1-b_2) \in B$. По лемме 3.1, $A+B$ – левый идеал. Для правых и двусторонних идеалов доказательство аналогично. КД

Лемма 3.4. Если A – левый идеал, T – некоторое непустое множество элементов кольца R, то AT – левый идеал R.

Д Возьмем два элемента из AT:

$$x=a_1t_1+\ldots+a_kt_k \in AT,\ a_i \in A,\ t_i \in T,$$

$$y=a'_1t'_1+\ldots+a'_nt'_n \in AT,\ a'_i \in A,\ t'_i \in T.$$

Тогда $x-y=\sum_{i=1}^{k} a_it_i+\sum_{i=1}^{n} a'_it'_i \in AT$. Если $r \in R$, то $ra_i \in A$ для всех $i=1,2,\ldots,k$, значит, $rx=\sum_{i=1}^{k}(ra_i)t_i \in AT$. По лемме 3.1, AT – левый идеал. КД

Из леммы 3.4 вытекает, что произведение Aa левого идеала A на элемент $a \in R$ является левым идеалом кольца R. В частности, Ra есть левый идеал.

Аналогично лемме 3.4 доказывается

Лемма 3.5. Если A – правый идеал, T – некоторое непустое множество элементов кольца R, то TA – правый идеал R.

Следствием лемм 3.4 и 3.5 является

Лемма 3.6. Если A – левый, правый или двусторонний идеал кольца R, то для любого натурального n степень A^n является соответственно левым, правым или двусторонним идеалом

кольца R.

Поскольку по теореме I.I пересечение любого семейства подмодулей снова является подмодулем, то пересечение любого семейства левых, правых или двусторонних идеалов является соответственно левым, правым или двусторонним идеалом. Это позволяет ввести следующее определение.

Пусть M – некоторое множество элементов кольца R. Заметим, что кольцо R является идеалом, содержащим M. Пересечение всех левых идеалов, содержащих M, обозначается через $(M>$ и называется левым идеалом, порожденным множеством M. Пересечение всех правых идеалов, содержащих M, обозначается через $<M)$ и называется правым идеалом, порожденным множеством M. Пересечение всех идеалов, содержащих M, обозначается через (M) и называется идеалом, порожденным множеством M.

Если множество M состоит из одного элемента, то мы приходим к понятию главного идеала. А именно, идеалы вида $<a), (a>$ и (a), где $a\in R$, называются главными. Структура главных идеалов проясняется следующей теоремой.

Теорема 3.2. Пусть a – произвольный элемент кольца R. Тогда $(a>=Ra+\mathbb{Z}a$, $<a)=aR+a\mathbb{Z}$, $(a)=RaR+\mathbb{Z}a+Ra+aR$.

▯ Так как $(a>$ – левый идеал, то $Ra\subseteq(a>$. Так как $(a>$ – подгруппа аддитивной группы кольца R, то $\mathbb{Z}a\subseteq(a>$. Значит, $Ra+\mathbb{Z}a\subseteq(a>$. Пусть теперь x_1 и x_2 – любые элементы из $Ra+\mathbb{Z}a$. Тогда $x_i=r_ia+n_ia$, $r_i\in R$, $n_i\in\mathbb{Z}$, $i=1,2$. Очевидно, $x_1-x_2=(r_1-r_2)a+(n_1-n_2)a\in Ra+\mathbb{Z}a$. Если $r\in R$, то $rx_1=(rr_1+n_1r)a+0a\in Ra+\mathbb{Z}a$. По лемме 3.I, $Ra+\mathbb{Z}a$ – левый идеал. Так как $a=0a+1a\in Ra+\mathbb{Z}a$, то мы получаем требуемое равенство $(a>=Ra+\mathbb{Z}a$. Равенство $<a)=aR+a\mathbb{Z}$ устанавливается аналогично.

Установим справедливость третьего равенства. Правая его часть, как легко заметить, входит в (a) и является аддитивной подгруппой. Если $r\in R$, то $r(RaR)\subseteq RaR$, $(RaR)r\subseteq RaR$, так как $RaR=(Ra)R=R(aR)$ согласно леммам 3.4 и 3.5 является идеалом. Далее, $r(\mathbb{Z}a)\subseteq Ra$, $(\mathbb{Z}a)r\subseteq aR$, $r(Ra)\subseteq Ra$, $(Ra)r\subseteq RaR$, $r(aR)\subseteq RaR$, $(aR)r\subseteq aR$. Это показывает, что $RaR+\mathbb{Z}a+Ra+aR$ является идеалом, причем этот идеал содержит $a=0a0+1a+0a+a0$, а значит, совпадает с (a). ▯

Заметим, что левый идеал Ra может не совпадать с $(a>$, поскольку может не содержать a. Простейший пример: если R – кольцо четных целых чисел с обычными операциями сложения и умножения, то $2\notin R2=2R$.

Теорема 3.3. Пусть R – кольцо с единицей e. Тогда для любого $a\in R$ имеет место $(a>=Ra$, $<a)=aR$, $(a)=RaR$.

▯ Из того, что R имеет единицу e, вытекает следующее: $\mathbb{Z}a=(ae)a=a(e\mathbb{Z})\subseteq Ra\cap aR$, $Ra=Rae\subseteq RaR$, $aR=eaR\subseteq RaR$. Теперь применяем теорему 3.2. ▯

Обратим внимание на то, что нулевой идеал (0) является главным. Если кольцо R имеет единицу e, то оно само является главным идеалом, поскольку $(e)=R$.

Лемму 3.3 можно распространить на случай любого множества идеалов. Определим сумму $\sum_{i\in I}A_i$ подгрупп A_i аддитивной группы кольца R как множество всех конечных сумм $x_1+x_2+\ldots+x_k$, где $x_1, x_2, \ldots, x_k$ взяты из некоторых подгрупп A_i. Определим $(A_i\,|\,i\in I>$ как левый идеал, порожденный множеством $\bigcup_{i\in I}A_i$. Аналогично вводим $<A_i\,|\,i\in I)$, $(A_i\,|\,i\in I)$.

Теорема 3.4. Пусть дано некоторое множество $\{A_i\,|\,i\in I\}$ подгрупп аддитивной группы кольца R. Тогда:

1) $\sum_{i\in I}A_i=(A_i\,|\,i\in I>$, если A_i является левым идеалом для любого $i\in I$;

2) $\sum_{i\in I}A_i=<A_i\,|\,i\in I)$, если A_i является правым идеалом для любого $i\in I$;

3) $\sum_{i\in I}A_i=(A_i\,|\,i\in I)$, если A_i является идеалом для любого $i\in I$.

Доказательство очевидно.

5. Фактор-кольцо. Пусть K – идеал кольца R. Рассмотрим фактор-группу R/K аддитивной группы кольца R по подгруппе K. Элементы из R/K складываются по правилу

$$(a+K)+(b+K)=(a+b)+K. \qquad (1)$$

Введем операцию умножения элементов R/K следующим образом

$$(a+K)(b+K)=ab+K. \qquad (2)$$

Если $a+K=a'+K$, $b+K=b'+K$, то $a'=a+k_1$, $b'=b+k_2$, где $k_1, k_2 \in K$, причем $a'b'=ab+(ak_2+k_1b+k_1k_2)$ принадлежит $ab+K$, поскольку K – идеал. Значит, определение умножения (2) не зависит от выбора представителей смежных классов. Легко проверить, что R/K с операциями сложения (1) и умножения (2) является кольцом; это кольцо называется фактор-кольцом кольца R по идеалу K.

Теорема 3.5. Пусть K – идеал кольца R. Тогда отображение $\varphi: r \mapsto r+K$, где $r \in R$, является гомоморфизмом кольца R на фактор-кольцо R/K, причем $\ker\varphi = K$.

Доказательство очевидно. Гомоморфизм φ из теоремы 3.3 называют естественным.

Обратимся теперь к гомоморфизмам колец. Если дан кольцевой гомоморфизм $f: R \to R^*$, то нетрудная проверка показывает справедливость следующих утверждений:

а) если H – подкольцо из R, то его образ $H^f = \{a^f \mid a \in H\}$ является подкольцом кольца R^*;

б) 0^f есть нулевой элемент кольца R^*;

в) $(-a)^f = -a^f$ для любого $a \in R$;

г) если e – единица кольца R, то e^f – единица кольца R^*.

Докажем, что ядрами гомоморфизмов исчерпываются все идеалы кольца. Этот факт вытекает из теоремы 3.5 и следующей теоремы.

Теорема 3.6. Пусть дан гомоморфизм $f: R \to R^*$ кольца R на кольцо R^*. Тогда $\ker f$ – идеал кольца R и имеет место изоморфизм $R/\ker f \cong R^*$.

Доказательство. Поскольку f является гомоморфизмом аддитивной группы кольца R, то $\ker f$ является подгруппой и отображение $\varphi: x+\ker f \mapsto x^f$, где $x \in R$, является изоморфизмом аддитивной группы кольца $R/\ker f$ на аддитивную группу кольца R^*. Если $r \in R$, $k \in \ker f$, то $(rk)^f = r^f k^f = r^f 0 = 0$, $(kr)^f = k^f r^f = 0 r^f = 0$, т.е. $\ker f$ – идеал в R. Для любых $x, y \in R$ имеем

$$\varphi: xy+\ker f \mapsto (xy)^f = x^f y^f = (x+\ker f)^\varphi (y+\ker f)^\varphi$$

Значит, φ – кольцевой изоморфизм. КД

6. Описание неприводимых R-модулей. Если K – правый (левый) идеал кольца R, то поскольку K – подмодуль модуля R_R ($_RR$), фактор-группа R/K аддитивной группы кольца R является правым (левым) R-модулем (внимание: в данном случае R/K необязательно является кольцом).

Введем следующее определение. Максимальный по включению $\subseteq$ элемент множества всех отличных от R правых (левых) идеалов кольца R назовем максимальным правым (левым) идеалом кольца R. Другими словами, правый (левый) идеал K кольца R называется максимальным правым (левым) идеалом, если $K \neq R$ и K не содержится ни в каком другом отличном от R правом (левом) идеале кольца R.

Лемма 3.7. Пусть K – левый (правый) идеал кольца R. Тогда следующие утверждения эквивалентны:

1) левый (правый) R-модуль R/K неприводим;

2) K – максимальный левый (правый) идеал кольца R.

Д. Пусть дано 1), и пусть I – левый (правый) идеал кольца R, содержащий K и отличный от R. Тогда I/K является подмодулем R-модуля R/K, а так как последний неприводим, то I/K – нулевой подмодуль, т.е. $I = K$. Значит, верно 2).

Пусть дано 2). Пусть I/K – подмодуль левого (правого) R-модуля R/K. Но тогда I – левый (правый) идеал R. Так как $I \supseteq K$ и верно 2), то либо $I = R$, либо $I = K$, т.е. верно 1). КД

Будем использовать следующие обозначения. Если M – левый R-модуль и $a \in M$, то $Ra = \{ra \mid r \in R\}$, $A_R(M) = \{r \in R \mid ra = 0$ для всех $a \in M\}$. Если M – правый R-модуль и $a \in M$, то $aR = \{ar \mid r \in R\}$, $A_R(M) = \{r \in R \mid ar = 0$ для всех $a \in M\}$.

Теорема 3.7. Если M – левый (правый) неприводимый R-модуль и $A_R(M)\neq R$, то R обладает таким левым (правым) идеалом K, что выполняются следующие условия:

1) K – максимальный левый (правый) идеал кольца R;

2) существует такой элемент $a\in R$, что для всех $x\in R$ имеет место $x-xa\in K$. $(x-ax\in K)$.

Д Мы докажем теорему только для левых модулей, так как для правых доказательство аналогично. Пусть M – неприводимый левый R-модуль. Рассмотрим $S=\{u\in M \mid Ru=0\}$. Ясно, что S является подмодулем модуля M. Так как M неприводим и $A_R(M)\neq R$, то $S=0$. Отсюда следует, что $Rm\neq 0$ для любого ненулевого $m\in M$. Так как Rm – подмодуль неприводимого модуля M, то $Rm=M$. Определим теперь отображение $\varphi: r\mapsto rm$, $r\in R$. Ясно, что φ является гомоморфизмом модуля R в модуль M. Так как $Rm=M$, то φ – эпиморфизм. Его ядро $\operatorname{Ker}\varphi=\{x\in R \mid xm=0\}$ является левым идеалом кольца R. По теореме I.3 R-модули $R/\operatorname{Ker}\varphi$ и M изоморфны. Значит, левый R-модуль $R/\operatorname{Ker}\varphi$ неприводим, и по лемме 3.7 левый идеал K максимален.

Так как $Rm=M$, то $am=m$ для некоторого $a\in R$. Тогда для любого $x\in R$ имеем $xam=xm$, $(x-xa)m=0$. Следовательно, $x-xa\in\operatorname{Ker}\varphi$. КД

7. Нильпотентность. Пусть I – левый, правый или двусторонний идеал кольца R. Если $I^n=(0)$ для некоторого натурального n, то I называется нильпотентным левым, правым или двусторонним идеалом.

Согласно введенным ранее обозначениям, I^n состоит из конечных сумм элементов вида $a_1a_2\dots a_n$, где $a_i\in I$. Поэтому равенство $I^n=(0)$ эквивалентно тому, что все произведения элементов из I, содержащие n множителей, равны 0.

Элемент x кольца R называется нильпотентным, если $x^n=0$ для некоторого натурального n. Понятно, что все элементы нильпотентных левых, правых или двусторонних идеалов нильпотентны.

Лемма 3.8. Если a_1 и a_2 – нильпотентные элементы кольца R и $a_1a_2=a_2a_1$, то элементы $-a_1$, $-a_2$, a_1+a_2 также нильпотентны.

Д Пусть $a_1^m=a_2^n=0$ для некоторых натуральных чисел

m,n. Тогда $(-a_1)^m=(-1)^m a_1^m=0$ так что $-a_1$ нильпотентен. Пусть $m\geqslant n$, $t=2m$. Применим биномиальную формулу ([1], с.56):

$$(a_1+a_2)^t=\sum_{i=0}^{t}\binom{t}{i}a_1^{t-i}a_2^{i}.$$

Здесь в каждом слагаемом либо $t-i\geqslant m$, либо $i\geqslant m$. Поэтому ясно, что $(a_1+a_2)^t=0$. КД

Элемент x кольца R называется идемпотентом, если $x\neq 0$ и $x^2=x$. Из равенства $x^2=x$ следует $x^m=x$ для любого натурального m.

Понятно, что нильпотентный элемент не может быть идемпотентом. Поэтому нильпотентный левый идеал не содержит идемпотентов. Мы укажем условие, которое гарантирует существование идемпотентов у ненильпотентных левых идеалов. Таким условием является условие минимальности для левых идеалов. Говорят, что R – кольцо с условием минимальности для левых идеалов, если левый регулярный модуль ${}_RR$ удовлетворяет условию минимальности для подмодулей (иными словами, каждая убывающая цепь левых идеалов $I_1\supset I_2\supset\dots$ кольца R конечна). Аналогично вводится условие минимальности для правых идеалов.

Пример 3.3. Пусть $G=\{x_1=e,x_2,\dots,x_n\}$ – конечная группа порядка n, V – левое n-мерное линейное пространство над полем F с базисом $\{u_1,u_2,\dots,u_n\}$. Ввиду соответствия $x_i\mapsto u_i$, мы можем отождествить x_i с u_i и считать, что V – пространство с базисом $\{x_1,x_2,\dots,x_n\}$. Элементы из V складываются по правилу

$$\sum_{i=1}^{n}\alpha_i x_i+\sum_{i=1}^{n}\beta_i x_i=\sum_{i=1}^{n}(\alpha_i+\beta_i)x_i.$$

Введем умножение элементов из V следующим образом:

$$\Big(\sum_{i=1}^{n}\alpha_i x_i\Big)\Big(\sum_{j=1}^{n}\beta_j x_j\Big)=\sum_{i,j}(\alpha_i\beta_j)(x_i x_j).$$

Ясно, что множество элементов V с указанными операциями сложения и умножения является кольцом. Это кольцо обозначается через FG и называется групповым кольцом группы G над полем F. Кольцо FG имеет единицу $1e$, где 1 – единица поля F, e – единица группы G. Поскольку каждый левый идеал кольца FG является одновременно подпространством

пространства V, то FG удовлетворяет условию минимальности для левых идеалов.

Лемма 3.9. Если R – кольцо с условием минимальности для левых идеалов, то любое непустое множество левых идеалов кольца R имеет минимальный элемент.

Д Пусть дано непустое множество $\mathfrak{M}$ левых идеалов кольца R. Если левый идеал $I_1 \in \mathfrak{M}$ не является минимальным элементом $\mathfrak{M}$, то $I_1 \supset I_2$, где $I_2 \in \mathfrak{M}$. Если I_2 не минимален в $\mathfrak{M}$, то $I_2 \supset I_3$, где $I_3 \in \mathfrak{M}$. Продолжая этот процесс, мы получим убывающую цепь $I_1 \supset I_2 \supset \dots$, которая по условию обрывается на некотором номере n. Это значит, что $I_n \in \mathfrak{M}$, но не существует такого $I \in \mathfrak{M}$, что $I_n \supset I$. Значит, I_n – минимальный элемент $\mathfrak{M}$. КД

Минимальный элемент множества всех ненулевых левых идеалов кольца R называется минимальным левым идеалом кольца R. Ясно, что минимальный левый идеал кольца R – это неприводимый подмодуль левого регулярного модуля ${}_R R$.

Теорема 3.8. Пусть R – кольцо с условием минимальности для левых идеалов. Тогда каждый ненильпотентный левый идеал кольца R содержит идемпотент.

Д Пусть I – ненильпотентный левый идеал кольца R. По лемме 3.9, множество всех содержащихся в I ненильпотентных левых идеалов кольца R содержит минимальный элемент K. Таким образом, каждый левый идеал кольца R, строго содержащийся в K, нильпотентен.

По лемме 3.6 произведение KK является левым идеалом, причем $KK \subseteq K$. Если $KK \neq K$, то левый идеал KK нильпотентен, т.е. $(KK)^n = K^{2n} = (0)$, что невозможно. Итак,

$$KK = K \neq (0). \qquad (1)$$

Так как $KK \neq (0)$, то мы можем, ввиду леммы 3.9, выбрать в K наименьший левый идеал L кольца R, удовлетворяющий условию:

$$KL \neq (0). \qquad (2)$$

По лемме 3.4, KL – левый идеал. Из того, что L – левый идеал, следует $KL \subseteq L$. Таким образом,

$$KL \subseteq L \subseteq K \subseteq I. \qquad (3)$$

Из (2) вытекает, что найдется такой элемент x, что

$$Kx \neq (0), \quad x \in L. \qquad (4)$$

По лемме 3.4, Kx – левый идеал R, а так как x принадлежит левому идеалу L, то $Kx \subseteq L$. Если $Kx \subsetneq L$, то ввиду выбора L имеем $K(Kx) = Kx = (0)$, что противоречит (4). Значит,

$$Kx = L, \quad x \in L. \qquad (5)$$

Из (5) вытекает существование элемента $a \in K$ такого, что $ax = x$. Если $a^m = 0$ для некоторого натурального m, то $a^m x = ax = x = 0$, что невозможно, так как $x \neq 0$ согласно (4). Мы приходим к следующему: a ненильпотентен, содержится в K, причем $(a^2 - a)x = 0$.

Рассмотрим $N = \{u \in K \mid ux = 0\}$. Заметим, что N – левый идеал, причем из (4) вытекает, что $N \subset K$. Значит, N нильпотентен и все его элементы нильпотентны.

Рассмотрим элемент

$$n_1 = a^2 - a, \qquad (6)$$

принадлежащий N. Если $n_1 = 0$, то $a^2 = a$ – искомый идемпотент. Пусть $n_1 \neq 0$. Рассмотрим

$$a_1 = a + n_1 - 2an_1. \qquad (7)$$

Очевидно, $a_1 \in K$. Из (6) и (7) вытекает, что элементы a, a_1, n_1 попарно перестановочны. Поэтому если a_1 нильпотентен, то по лемме 3.8 элемент $a = a_1 - (n_1 - 2an_1)$ также нильпотентен (элемент $n_1 - 2an_1$ нильпотентен, так как принадлежит нильпотентному левому идеалу N). Значит, a_1 ненильпотентен. Строим элемент

$$n_2 = a_1^2 - a_1 = 4n_1^3 - 3n_1^2 \in N.$$

Если $n_2 = 0$, то a_1 – искомый идемпотент. Пусть $n_2 \neq 0$, тогда строим элемент $a_2 = a_1 + n_2 - 2a_1 n_2 \in K$ и устанавливаем его ненильпотентность. И так далее.

Если a_{i-1} уже построен, то $n_i = a_{i-1}^2 - a_{i-1}$ содержит в каждом слагаемом множитель $n_1^{2^{i-1}}$. Строим $a_i = a_{i-1} + n_i - 2a_{i-1}n_i$, тогда $n_{i+1} = a_i^2 - a_i = 4n_i^3 - 3n_i^2$ содержит в каждом слагаемом множитель $n_1^{2^i}$. Так как n_1 нильпотентен, то для достаточно большого i будет $n_1^{2^i} = 0$, но тогда $n_{i+1} = a_i^2 - a_i = 0$ и

a_i – искомый идемпотент из K. Так как $K \subseteq L$, то $a_i \in L$. КД

8. Радикал. Пусть R – кольцо с условием минимальности для левых идеалов. Сумму всех нильпотентных левых идеалов кольца R называют радикалом кольца R и обозначают через $\mathrm{rad}\,R$. Если $\mathrm{rad}\,R = (0)$, то кольцо R называют полупростым. В этом пункте мы установим основное свойство радикала.

Лемма 3.10. Сумма конечного числа нильпотентных левых (правых) идеалов кольца R является нильпотентным левым (правым) идеалом.

Д Пусть A, B – нильпотентные левые идеалы кольца R. Тогда $A^m = B^n = (0)$ для некоторых натуральных чисел m, n. Согласно введенному в п.4 определению произведения множеств элементов кольца, $(A+B)^{m+n}$ состоит из конечных сумм элементов вида $x_1 x_2 \dots x_{m+n}$, где $x_i \in A+B$. Пусть $x_i = x_i' + x_i''$, $x_i' \in A$, $x_i'' \in B$, $i = 1, 2, \dots, m+n$. Тогда $x_1 x_2 \dots x_{m+n}$ запишется в виде суммы, в которой каждое слагаемое одного из следующих двух типов:

$$\dots x'_{i_1} \dots x'_{i_2} \dots x'_{i_m} \dots,$$
$$\dots x''_{j_1} \dots x''_{j_2} \dots x''_{j_n} \dots,$$

где точками обозначены некоторые элементы. Поскольку A и B – левые идеалы, то в указанных слагаемых $\dots x'_{i_k} \in A$, $\dots x''_{j_k} \in B$. Так как A и B – нильпотентны, то произведение любых m элементов из A равно 0, а также произведение любых n элементов из B равно 0. Значит, $x_1 x_2 \dots x_{m+n} = 0$ что и доказывает нильпотентность $A+B$. Для правых идеалов доказательство аналогично. КД

Теорема 3.9. Пусть R – кольцо с условием минимальности для левых идеалов. Тогда справедливы следующие утверждения:

1) $\mathrm{rad}\,R$ – нильпотентный идеал кольца R;

2) $\mathrm{rad}\,R$ содержит все нильпотентные правые идеалы кольца R;

3) кольцо $R/\mathrm{rad}\,R$ полупросто.

Д По теореме 3.4, $N = \mathrm{rad}\,R$ есть левый идеал кольца R. Предположим, что N ненильпотентен. Тогда по теореме 3.8 в N имеется идемпотент a. По определению суммы (см.п.4), $a = x_1 + x_2 + \dots + x_t$, где x_i принадлежит нильпотентному левому идеалу N_i кольца R, $i = 1, 2, \dots, t$. По лемме 3.10, левый идеал $N_1 + N_2 + \dots + N_t$ нильпотентен, а значит, элемент a нильпотентен. Противоречие. Итак, N – нильпотентный левый идеал.

По лемме 3.4 и 3.5, NR – двусторонний идеал. Для любого $t \geq 1$, используя ассоциативность умножения множеств и то, что $RN \subseteq N$, получаем:

$$(NR)^t = N(RN)^{t-1}R \subseteq NN^{t-1}R = N^tR.$$

Теперь ясно, что из нильпотентности N следует нильпотентность идеала NR. Так как N содержит все нильпотентные левые идеалы, то $NR \subseteq N$. Последнее включение показывает, что N – правый идеал, т.е. 1) доказано.

Пусть I – нильпотентный правый идеал кольца R. По лемме 3.4 и 3.5, RI – идеал. Для любого $t > 1$ имеем $(RI)^t = R(IR)^{t-1}I \subseteq RI^t$. Значит, идеал RI нильпотентен. По лемме 3.10, $I+RI$ является нильпотентным правым идеалом. Так как $r(I+RI) \subseteq RI \subseteq I+RI$ для любого $r \in R$, то $I+RI$ – левый идеал. Тогда $I \subseteq I+RI \subseteq N$, и 2) доказано.

Пусть A/N – нильпотентный левый идеал R/N. Тогда $(A/N)^k = N$, т.е. $A^k \subseteq N$. Поэтому из $N^t = (0)$ получаем $A^{kt} \subseteq N^t = (0)$ и $A = N$. Значит, в R/N нет ненулевых нильпотентных идеалов. Кроме того, R/N удовлетворяет условию минимальности для левых идеалов. Мы видим, что 3) верно. КД

9. Полупростые кольца. Займемся выяснением свойств полупростых колец. Подчеркнем, что по определению полупростое кольцо удовлетворяет условию минимальности для левых идеалов.

Лемма 3.11. Пусть A – ненулевой левый идеал полупростого кольца R. Тогда $A = Ra = (a)$ для некоторого идемпотента a из A.

Д Так как R полупросто, то A ненильпотентен. По теореме 3.8 множество S всех идемпотентов из A не пусто. Каждому элементу $a \in S$ поставим в соответствие множество

$A(a)=\{x\in A \mid xa=0\}$. Ясно, что $A(a)$ – левый идеал кольца R . По лемме 3.9 множество $\{A(a)\mid a\in S\}$ имеет минимальный элемент $A(a_0)$. Рассмотрим два случая.

Предположим, что $A(a_0)\neq(0)$. Так как $A(a_0)$- ненулевой левый идеал полупростого кольца R , то по теореме 3.8 $A(a_0)$ содержит идемпотент a_1 . По построению, $a_1\in A$, $a_1a_0=0$.Рассмотрим элемент $b=a_0+a_1-a_0a_1\in A$. Вычисляя b^2 , получаем, что $b^2=b$. Кроме того, $a_1b=a_1$. Отсюда следует, что $b\neq 0$. Таким образом, b – идемпотент. Пусть $x\in A(b)$, т.е. $xb=0$. Тогда $xba_0=0$. Но $ba_0=a_0$, следовательно, $xa_0=0$. Последнее означает, что $x\in A(a_0)$. Тем самым установлено, что $A(b)\subseteq A(a_0)$. Так как $a_1b=a_1\neq 0$, то $a_1\notin A(b)$. Так как $a_1\in A(a_0)$, то мы получаем $A(b)\subset A(a_0)$. Но это противоречит минимальности $A(a_0)$. Таким образом, случай $A(a_0)\neq(0)$ невозможен.

Пусть $A(a_0)=(0)$. Для любого $x\in A$ имеем $(x-xa_0)a_0=0$. Поэтому $x-xa_0\in A(a_0)=(0)$, т.е. $x=xa_0$. Значит, $A=Aa_0\subseteq Ra_0$. Так как $a_0\in A$ и A – левый идеал, то $Ra_0\subseteq A$. Следовательно, $A=Ra_0$. ☐

Обозначим через $Z(R)$ множество всех тех элементов кольца R , которые перестановочны с каждым элементом кольца R . Множество $Z(R)$ называют центром кольца R . Если $a\neq 0$, $a^2=a\in Z(R)$, то a называется центральным идемпотентом кольца R .

Лемма 3.12. Пусть A – ненулевой идеал полупростого кольца R . Тогда $A=aR=Ra=(a)$, где a – идемпотент из $Z(R)$. В частности, a – единица кольца A .

▲ По лемме 3.11, $A=(a>=Ra$, где $a^2=a\neq 0$. Рассмотрим множество $B=\{x-ax \mid x\in A\}$. Очевидно, $B\subseteq A$. Ясно также, что B – правый идеал кольца R . Так как $aB=(0)$ и $Aa=Ra^2=A$, то $B^2\subseteq AB\subseteq AaB=(0)$. Ввиду теоремы 3.9, отсюда следует $B=(0)$. Значит, $x=ax$ для любого $x\in A$. Любой элемент $x\in A$ представим в виде $x=ra$, где $r\in R$ и так как $a^2=a$, то $xa=x$. Таким образом, a – единица кольца A . Получаем теперь:

$$A=aA\subseteq aR\subseteq A,\quad A=aR.$$

Если $x\in R$, то $xa\in A$, $ax\in A$. Так как a – единица в A , то $axa=ax=xa$. Значит, $a\in Z(R)$. ☐

При $A=R$ из леммы 3.12 получаем следующий результат.

Лемма 3.13. Всякое полупростое кольцо обладает единицей.

Наша очередная цель состоит в том, чтобы доказать полную приводимость левого регулярного модуля ${}_RR$, где R – полупростое кольцо. В связи с этим фактом мы будем иметь возможность применить результаты п.4 § 2 в аддитивной записи. Отметим, что для обозначения прямой суммы мы будем использовать знак $\dot{+}$.

Теорема 3.10. Следующие утверждения относительно кольца R эквивалентны:

1) R полупросто;

2) R обладает единицей и удовлетворяет условию минимальности для левых идеалов, а левый регулярный модуль ${}_RR$ вполне приводим.

▲ Пусть R – полупростое кольцо и A – его произвольный левый идеал. По лемме 3.11, $A=Ra$ для некоторого $a=a^2\in A$ По лемме 3.13, R имеет единицу e . По лемме 3.4, $B=R(e-a)$ есть левый идеал. Если $r\in R(e-a)\cap Ra$, то $r=r_1(e-a)=r_2a$, где $r_1,r_2\in R$. Тогда $ra=r_2a^2=r_2a=r$, $ra=r_1(e-a)a=0$, откуда $r=0$. Это означает, что $Ra\cap R(e-a)=(0)$. Так как каждый элемент $x\in R$ представим в виде $x=xa+x(e-a)$, то ясно, что $R=Ra\dot{+}R(e-a)$. Итак, из 1) следует 2).

Пусть теперь дано 2). Так как $\mathrm{rad}\,R$ является подмодулем вполне приводимого модуля ${}_RR$, то $R=\mathrm{rad}R\dot{+}K$, где K – левый идеал. По условию ${}_RR$ имеет единицу e . Представим e в виде $e=x+y$, где $x\in\mathrm{rad}R$, $y\in K$. Так как

$$x-x^2=x(e-x)=(e-x)x=xy=yx\in\mathrm{rad}R\cap K=(0),$$

то $x-x^2=0$. Так как по теореме 3.9 $\mathrm{rad}R$ нильпотентен, то x не может быть идемпотентом. Значит, $x=0$, $e=y\in K$, отсюда следует $K=R$. Таким образом, из 2) следует 1). ☐

Из теоремы 3.10 и следствия 2.4.1 получаем

Следствие 3.10.1. Полупростое кольцо удовлетворяет условию максимальности для левых идеалов.

Следствие 3.10.2. Полупростое кольцо $R\neq(0)$ представимо в виде такой прямой суммы главных левых идеалов

$R = Re_1 \dot{+} Re_2 \dot{+} \ldots \dot{+} Re_n$, что выполняются следующие условия:

1) Re_i - минимальный левый идеал кольца R , e_i - идемпотент, $i = 1, 2, \ldots, n$;

2) $e_i e_j = 0$ для любых $i \neq j$.

Д Согласно следствию 2.4.2, R представимо в виде прямой суммы конечного числа минимальных левых идеалов: $R = L_1 \dot{+} L_2 \dot{+} \ldots \dot{+} L_n$. Представим единицу e кольца R в виде $e = e_1 + e_2 + \ldots + e_n$, где $e_i \in L_i$. Тогда $e_j e = e_j = e_j e_1 + e_j e_2 + \ldots + e_j e_n$. Так как $e_j e_i \in L_i$, а сумма $R = L_1 \dot{+} L_2 \dot{+} \ldots \dot{+} L_n$ прямая, то $e_j e_1 = 0, e_j e_2 = 0, \ldots, e_j e_j = e_j, e_j e_{j+1} = 0, \ldots, e_j e_n = 0$. Отсюда получаем: $e_i e_j = 0$ при $i \neq j$, $e_i e_i = e_i$. Из $e = e_1 + e_2 + \ldots + e_n$ выводим $Re = R = Re_1 \dot{+} Re_2 \dot{+} \ldots \dot{+} Re_n$, где $Re_i \subseteq L_i$. Из минимальности L_i следует, что либо $Re_i = 0$, либо $Re_i = L$. Нетрудно заметить (прямая сумма!), что случай $Re_i = (0)$ невозможен. КД

Замечание: идемпотенты $e_1, e_2, \ldots, e_n$, удовлетворяющие условию 2) следствия 3.10.2, называются ортогональными.

Следствие 3.10.3. Если кольцо $R \neq (0)$ полупросто, то каждый неприводимый левый R-модуль изоморфен некоторому минимальному левому идеалу кольца R .

Д Кольцо R обладает единицей $e \neq 0$ и представимо в виде прямой суммы минимальных левых идеалов: $R = L_1 \dot{+} L_2 \dot{+} \ldots \dot{+} L_n$. Пусть M - неприводимый левый R-модуль. Из существования единицы $e \neq 0$ следует, что $A_R(M) \neq R$. По теореме 3.7, R обладает таким максимальным левым идеалом K , что левые R-модули R/K и M изоморфны. Ясно, что $K \dot{+} L_i = R$ для некоторого i . По теореме I.5, левые R-модули R/K и L_i изоморфны. КД

Ненулевое кольцо R называется телом, если множество всех ненулевых элементов из R составляет группу относительно операции умножения.

Теорема 3.II. Главный левый идеал $(a\rangle$ полупростого кольца R , порожденный идемпотентом a , минимален тогда и только тогда, когда кольцо aRa - тело.

Д Согласно введенным обозначениям, xRx состоит из всех элементов вида $x\tau x$, где $\tau \in R$.Поэтому xRx

является подкольцом кольца R для любого $x \in R$. Согласно лемме 3.I3, R обладает единицей e .

Пусть L - минимальный левый идеал кольца R . Согласно лемме 3.II, $L = (a\rangle = Ra$, где a - идемпотент. Очевидно, a является единицей кольца $D = aRa$. Пусть d - ненулевой элемент из D . Тогда Dd является главным левым идеалом кольца D и

$$R(Dd) \subseteq RD = R(aRa) \subseteq Ra = L.$$

Очевидно, $d \in R(Dd)$, причем по лемме 3.4 $R(Dd)$ есть левый идеал кольца R . Ввиду минимальности L имеем $R(Dd) = L$. Так как $a^2 = a$, то $D = aRa = aL = aRDd = aRaRad = (aRa)(aRa)d \subseteq (aRa)d = Dd$,

откуда $D = Dd$. Значит, найдется такой элемент $d_1 \in D$, что $a = d_1 d$. Тем самым и доказано, что D - тело. КД

Исследуем вопрос об изоморфизме минимальных левых идеалов полупростого кольца. При этом под изоморфизмом левых идеалов мы будем понимать их изоморфизм как левых R-модулей (подмодулей левого регулярного модуля ${}_R R$).

Лемма 3.I4.Если минимальные левые идеалы A и B полупростого кольца $R \neq (0)$ изоморфны, то $AB = B$ для некоторого $b \in B$.

Д Согласно лемме 3.II, $A = Ra = (a\rangle, a^2 = a$. Пусть α - K-изоморфизм A на B. Тогда $(\tau a)^\alpha = \tau a^\alpha$ для любого $\tau \in R$. Для любого $x \in A$ имеем $xa = x$, так как $A = Ra$ и $a^2 = a$. Поэтому $(xa)^\alpha = x^\alpha = xa^\alpha$, где $x \in A, x^\alpha \in B$. Отсюда и получаем $B = Aa^\alpha$. КД

Лемма 3.I5. Пусть A - минимальный левый идеал полупростого кольца $R \neq (0)$. Тогда для любого $\tau \in R$ справедливо следующее утверждение: либо $A\tau = (0)$, либо левые идеалы A и $A\tau$ изоморфны.

Д Пусть $\tau \in R$. По лемме 3.4, $A\tau$ - левый идеал R . Рассмотрим отображение $\varphi : m \mapsto m\tau, m \in A$. Очевидно, φ является эпиморфизмом левого R-модуля A на левый R-модуль $A\tau$. По теореме I.3, левые R-модули $A/\mathrm{Ker}\,\varphi$ и $A\tau$ изоморфны. Из минимальности A теперь следует, что либо $\mathrm{Ker}\,\varphi = A$ и $A\tau = (0)$ либо $\mathrm{Ker}\,\varphi = (0)$ и $A \cong A\tau$. КД

Лемма 3.I5. Пусть A и B - минимальные левые идеалы

полупростого кольца $R\neq(0)$. Если A и B изоморфны, то $AB=B$. Если же левые идеалы A и B не изоморфны, то $AB=(0)$.

Д Пусть A и B изоморфны. По лемме 3.14 $Ab=B$, $b\in B$. Отсюда следует $AB=B$ ..

Пусть теперь левые идеалы A и B неизоморфны. Тогда ввиду леммы 3.15 имеем $Ab=(0)$ для любого $b\in B$, а значит, $AB=(0)$. КД

Лемма 3.17. Пусть A – минимальный левый идеал полупростого кольца $R\neq(0)$. И пусть B – сумма всех тех левых идеалов кольца R, которые изоморфны A. Тогда B – двусторонний идеал кольца R.

Д По теореме 3.4, B – левый идеал. Пусть $b\in B$. Тогда $b=a_1+a_2+\ldots+a_m$, где a_i принадлежит левому идеалу L_i, изоморфному A. Пусть $r\in R$. Так как $a_i r\in L_i r$ и по лемме 3.15 либо $L_i r=(0)$, либо $L_i r\cong L_i\cong A$, то ясно, что $br\in B$. Значит, B – идеал. КД

Ненулевое кольцо S называется простым кольцом, если S полупросто и не содержит никаких двусторонних идеалов, кроме (0) и S. По определению, простое кольцо удовлетворяет условию минимальности для левых идеалов.

Теорема 3.I2 (первая теорема Молина-Веддербарна). Каждое полупростое кольцо $R\neq(0)$ разлагается в прямую сумму идеалов, являющихся простыми кольцами.

Д Согласно следствию 3.10.2 кольцо R представимо в виде прямой суммы минимальных левых идеалов:

$$R=L_1\dot{+}L_2\dot{+}\ldots\dot{+}L_n. \qquad (1)$$

Пусть $L_t^*=\sum_{i=1}^{t}L_i$. Поскольку ряд $(0)\subset L_1^*\subset L_2^*\subset\ldots\subset L_n^*$ является R-композиционным рядом левого регулярного модуля ${}_RR$, то по теореме I.7 каждый минимальный левый идеал кольца R изоморфен одному L_i. Будем считать, что в разложении (I) слагаемые расположены таким образом, что первые m левых идеалов $L_1,\ldots,L_m$ попарно неизоморфны, а каждый из последующих левых идеалов L_i, $i>m$ изоморфен одному из $L_1,\ldots,L_m$. Пусть B_i – сумма всех тех левых идеалов кольца R, которые изоморфны L_i $(1\le i\le m)$. По лемме 3.17, B_i является идеалом. По лемме 3.16, $B_iB_j\neq(0)$ тогда и только тогда, когда $i=j$. Из (I) и способа построения идеалов B_i вытекает

$$R=B_1+B_2+\ldots+B_m. \qquad (2)$$

Покажем, что сумма (2) прямая. Для этого надо установить, что $C=B_i\cap\sum_{j\neq i}B_j=(0)$. Так как $B_iB_j=B_jB_i=(0)$ при $i\neq j$, то $B_iC=(0)$, $(\sum_{j\neq i}B_j)C=(0)$. Отсюда и из (I) получаем, что $RC=(0)$, а так как R обладает единицей $e\neq0$, то $C=(0)$. Итак, сумма (2) прямая.

Пусть L и I – соответственно левый идеал и двусторонний идеал кольца B_k, $1\le k\le m$. Если $r\in R$, то $r=b_1+\ldots+b_m$, где $b_i\in B_i$. Так как $B_iB_k=B_kB_i=(0)$ при $i\neq k$, то $b_iL=b_rI=Ib_i=(0)$ при $i\neq k$. Ввиду этого, $rL=b_kL\subseteq L$, $rI=b_kI\subseteq I$, $Ir=Ib_k\subseteq I$. Таким образом, L и I соответственно левый идеал и идеал кольца R. Мы установили, что идеалы и левые идеалы кольца B_k являются соответственно идеалами и левыми идеалами кольца R. Отсюда вытекает, что $\mathrm{rad}\,B_k\subseteq\mathrm{rad}\,R=(0)$ и B_k удовлетворяет условию минимальности для левых идеалов, т.е. кольцо B_k полупросто. Если идеал I кольца B_k не равен (0), то в I содержится минимальный левый идеал кольца R, а значит, и все левые идеалы вида Sx, где $x\in R$. Последнее означает, ввиду леммы 3.14, что в I входят все левые идеалы кольца R, изоморфные S, т.е. $S=B_k$. Тем самым доказано, что B_k – простое кольцо, $i=1,2,\ldots,m$. КД

Идеал B полупростого кольца $R\neq(0)$ называется его простой компонентой, если B есть сумма всех левых идеалов кольца R, изоморфных некоторому фиксированному минимальному левому идеалу кольца R. Информацию о простых компонентах, полученную в процессе доказательства теоремы 3.12, мы приведем в виде отдельного результата.

Теорема 3.I3. Пусть $B_1, B_2,\ldots,B_m$ – все различные простые компоненты полупростого кольца $R\neq(0)$. Тогда справедливы следующие утверждения:

1) B_i является простым кольцом, а также идеалом кольца R, $i=1,2,\ldots,m$;

2) $R=B_1\dot{+}B_2\dot{+}\ldots\dot{+}B_m$;

3) два минимальных левых идеала кольца R изоморфны тогда и только тогда, когда они принадлежат одной простой компоненте кольца R.

Простая компонента полупростого кольца $R\neq(0)$ является

минимальным идеалом, т.е. минимальным элементом множества всех ненулевых идеалов кольца R. Из следующей теоремы вытекает, что верно и обратное.

Теорема 3.14. Если I – ненулевой идеал полупростого кольца R, то I есть сумма некоторых простых компонент кольца R.

Д. Пусть L – минимальный левый идеал кольца R, содержащийся в I. И пусть B – простая компонента кольца R, содержащая L. Тогда $B=\sum_{x\in R} Lx$, и так как I – идеал, то ясно, что $B\subseteq I$. Пусть S – сумма всех простых компонент кольца R, содержащихся в I. По теореме 3.10, ${}_RR$ вполне приводим, а согласно лемме 2.12 вполне приводимым будет и его подмодуль I. Это значит, что $I=S\dotplus K$, где K – левый идеал кольца R. Если $K\neq(0)$, то в K содержится некоторый минимальный левый идеал A кольца R. Но тогда в I входит и простая компонента кольца R, содержащая A. Значит, $K=(0)$. ЧТД

Из теоремы 3.14 вытекает, что ненулевое полупростое кольцо имеет единственное разложение в прямую сумму идеалов, являющихся простыми кольцами.

10. Векторные пространства над телами. Пусть D – некоторое тело. Всякий левый D-модуль называется левым векторным пространством над телом D. Многие результаты о векторных пространствах над полями справедливы и для векторных пространств над телами (см. [3,4]). Так, совершенно ясно, как вводятся понятия линейной зависимости и независимости элементов пространства, базиса, подпространства и др.

Пусть дано левое n-мерное векторное пространство M над телом D. Пусть $u_1,\dots,u_n$ – базис этого пространства. Каждый элемент $x\in M$ единственным образом представим в виде $x=\alpha_1u_1+\dots+\alpha_nu_n$, где $\alpha_i\in D$. Если $\mathcal{A}$ – линейное преобразование пространства M (иначе, D-эндоморфизм аддитивной группы M), то $x\mathcal{A}=\alpha_1(u_1\mathcal{A})+\dots+\alpha_n(u_n\mathcal{A})$. Таким образом, линейное преобразование полностью определяется заданием образов элементов базиса. Если $u_i\mathcal{A}=\alpha_{i1}u_1+\alpha_{i2}u_2+\dots+\alpha_{in}u_n$, то матрица (α_{ij}) называется матрицей линейного преобразования $\mathcal{A}$ в базисе $u_1,\dots,u_n$.

Множество End_DM всех линейных преобразований левого векторного пространства M над телом D образует, очевидно, подкольцо кольца $End\,M$ всех эндоморфизмов аддитивной группы этого пространства. Обозначим через f функцию, ставящую в соответствие линейному преобразованию его матрицу в базисе $u_1,\dots,u_n$. Если $\mathcal{A},\mathcal{B}\in End_DM$, $f(\mathcal{A})=(\alpha_{ij})$, $f(\mathcal{B})=(\beta_{ij})$, $f(\mathcal{AB})=(\gamma_{ij})$, то

$$f(\mathcal{A}+\mathcal{B})=(\alpha_{ij})+(\beta_{ij})=(\alpha_{ij}+\beta_{ij}), \quad (1)$$

$$\gamma_{ij}=\sum_{k=1}^{n}\alpha_{ik}\beta_{kj}. \quad (2)$$

Равенство (2) показывает, что линейному преобразованию $\mathcal{AB}$ соответствует произведение матриц $(\alpha_{ij})(\beta_{ij})$. Таким образом, из (1) и (2) вытекает, что f – изоморфное отображение кольца End_DM на кольцо D_n всех матриц размера $n\times n$ над телом D.

Рассмотрим кольцо D_n подробнее. Его единицей служит единичная матрица E. Превратим кольцо D_n в левое векторное пространство над телом D, полагая $\beta(\alpha_{ij})=(\beta\alpha_{ij})$, где $\beta\in D$, $(\alpha_{ij})\in D_n$. Обозначим через E_{ij} такую матрицу из D_n, у которой на пересечении i-той строки и j-того столбца стоит единица e тела D, а на остальных местах нули. Каждая матрица $(\alpha_{ij})\in D_n$ представима в виде суммы $\sum\alpha_{ij}E_{ij}$. Следовательно, множество матриц E_{ij}, $1\le i,j\le n$, является базисом пространства D_n над D. Размерность этого пространства равна, таким образом, n^2. Базисные элементы перемножаются следующим образом

$$E_{ij}E_{jk}=E_{ik},\ E_{ij}E_{sk}=O,\ j\neq s. \quad (3)$$

Левые идеалы кольца D_n являются подпространствами. Поскольку нетривиальные подпространства имеют меньшую размерность, чем само пространство, то ясно, что D_n удовлетворяет условию минимальности для левых идеалов. Левый идеал D_nE_{ii} состоит, очевидно, из всех таких матриц, у которых в j-тых столбцах при $j\neq i$ стоят нули. Ясно, что кольцо D_n разлагается в прямую сумму левых идеалов

$$D_n=D_nE_{11}\dotplus D_nE_{22}\dotplus\dots\dotplus D_nE_{nn}. \quad (4)$$

Положим, что в (4) все слагаемые являются минимальными левыми идеалами. Пусть ненулевой левый идеал L кольца D_n содержится в D_nE_{tt}. Если (α_{ij}) – ненулевая матрица из L, то

$\alpha_{st} \neq 0$ для некоторого s. В теле найдется такой элемент x, что $x\alpha_{st} = e$ - единица тела D. Тогда

$$xE_{ts}(\alpha_{ij}) = xE_{ts}(\Sigma_i \alpha_{it} E_{it}) = x\alpha_{st} E_{tt} = E_{tt}.$$

Так как L - левый идеал, то отсюда следует, что $E_{tt} \subset L$, а значит, $L = D_n E_{tt}$. Итак, все слагаемые в (4) являются минимальными левыми идеалами, т.е. левый регулярный модуль D_n^n вполне приводим. По теореме 3.10, кольцо D_n полупросто.

Так как $E_{ji} = E_{jj}E_{ji}E_{ii} \in (D_n E_{jj})(E_{ii} D_n)$, то по лемме 3.16 все левые идеалы в разложении (4) между собой изоморфны (как левые D_n-модули). Значит, по теореме 3.13, D_n - простое кольцо. Мы пришли к следующей теореме.

Теорема 3.15. Для любого тела D и любого натурального числа n кольцо D_n является простым кольцом. Кроме того, n есть число слагаемых в разложении кольца D_n в прямую сумму минимальных левых идеалов.

II. Кольцо эндоморфизмов прямой суммы модулей. Пусть M - левый R-модуль. Эндоморфизм модуля M - это R-эндоморфизм его аддитивной группы. Множество всех эндоморфизмов левого R-модуля M обозначается через $End_R M$. Ясно, что $End_R M$ является подкольцом кольца $End\, M$ всех эндоморфизмов аддитивной группы M.

Лемма 3.18 (лемма Шура). Пусть M - неприводимый левый R-модуль. Тогда $End_R M$ - тело.

Д Кольцо $D = End_R M$ содержит единицу - тождественный автоморфизм. Пусть $f \in End_R M$. Тогда $Ker\, f$ и $Im\, f$ являются подмодулями модуля M. Если эндоморфизм f ненулевой, то из неприводимости M следует, что $Ker f = (0)$, $Im f = M$, т.е. f является автоморфизмом. Но тогда существует обратный автоморфизм $f^{-1} \in End_R M$, что и доказывает лемму. КД

Аналогично доказывается и следующая

Лемма 3.19. Пусть дан гомоморфизм f неприводимого левого R-модуля A в неприводимый левый R-модуль B. Тогда либо $Ker f = A$, либо f — изоморфизм.

Теорема 3.16. Пусть левый R-модуль M разлагается в прямую сумму неприводимых изоморфных подмодулей:

$$M = M_1 \dotplus M_2 \dotplus \dots \dotplus M_n, \quad n \geqslant 1.$$

Тогда кольцо $End_R M$ изоморфно кольцу D_n, где $D = End_R M_1$ — тело.

Д Пусть φ_i - проектирование модуля M в модуль M_i. По лемме 2.1, φ_i - эндоморфизм модуля M. Сумма всех проектирований φ_i совпадает с тождественным автоморфизмом:

$$\varepsilon = \varphi_1 + \varphi_2 + \dots + \varphi_n. \qquad (1)$$

Таким образом, каждый элемент $\mu \in End_R M$ представим в виде

$$\mu = \varepsilon\mu\varepsilon = (\Sigma_{i=1}^n \varphi_i)\mu(\Sigma_{i=1}^n \varphi_i) = \Sigma_{i,j} \varphi_i \mu \varphi_j.$$

Введем обозначение:

$$\varphi_i \mu \varphi_j = \mu_{ij} \qquad (2)$$

Тогда

$$\mu = \Sigma_{i,j} \mu_{ij}. \qquad (3)$$

Гомоморфизм μ_{ij} отображает модуль M_i в модуль M_j, а все $\varphi_k \mu \varphi_s$ $(k \neq i)$ - в нулевой подмодуль. Поэтому μ_{ij} - гомоморфизм модуля M_i в модуль M_j.

Обозначим H_{ij} множество всех гомоморфизмов модуля M_i в M_j. Ясно, что $\beta_{ij} \in H_{ij}$, то можно считать, что β_{ij} является эндоморфизмом модуля M, который отображает M_i в M_j, а β_{ks} $(k \neq i)$ - в нулевой подмодуль. Обозначим через K множество всех матриц (β_{ij}) размера $n \times n$ с элементами $\beta_{ij} \in H_{ij}$.

Доказывается, что эндоморфизму μ соответствует матрица $(\mu_{ij}) \in K$. Обратно, если $(\beta_{ij}) \in K$, то $\Sigma_{i,j} \beta_{ij}$ является эндоморфизмом модуля M. Если $\mu = \Sigma_{i,j} \mu_{ij} = \Sigma_{i,j} \beta_{ij}$, то $\varphi_k \mu \varphi_s = \mu_{ks} = \Sigma_{i,j} \varphi_k \beta_{ij} \varphi_s = \beta_{ks}$. Следовательно, мы построили взаимно однозначное отображение $f: \mu \longmapsto (\mu_{ij})$, $\mu \in End_R M$, $(\mu_{ij}) \in K$.

Если $f: \mu \longmapsto (\mu_{ij})$, $f: \beta \longmapsto (\beta_{ij})$, то учитывая, что $\mu_{ks}\beta_{zt} = 0$ при $s \neq z$, получаем:

$$\mu + \beta = \Sigma_{i,j} (\mu_{ij} + \beta_{ij}),$$
$$\mu\beta = \Sigma_{i,j} (\Sigma_k \mu_{ik} \beta_{kj}).$$

Эти равенства показывают, что эндоморфизму $\mu+\beta$ соответствует сумма матриц $(\mu_{ij})+(\beta_{ij})$, а эндоморфизму $\mu\beta$ – произведение матриц $(\mu_{ij})(\beta_{ij})$. Следовательно, f – изоморфизм кольца $End_R M$ на кольцо K (операциями в кольце K являются обычные операции сложения и умножения матриц).

По лемме 3.I8, $D=End_R M_1$ является телом. Пусть $(\mu_{ij})\in K$. Элемент μ_{11} содержится в D. Элемент μ_{KS} есть эндоморфизм, отображающий M_K в M_S, причем по лемме 3.I9 эндоморфизм μ_{KS} либо нулевой, либо является изоморфизмом модуля M_K на M_S. По условию, существуют такие $\mu_i\in H_{i1}(M_1,M_i)$, что $\mu_1=\varepsilon$, а для любого $i>1$ эндоморфизм μ_i является изоморфным отображением модуля M_i на M_1. Построим отображение $g: K\to D_n$ следующим образом:

$$g:(\mu_{ij})\longmapsto(\alpha_{ij}),\quad \alpha_{ij}=\mu_i^{-1}\mu_{ij}\mu_j.$$

То, что элемент $\alpha_{ij}=\mu_i^{-1}\mu_{ij}\mu_j$ принадлежит D, очевидно. Несложная проверка показывает, что g является изоморфизмом кольца K на кольцо D_n. Так как кольца $End_R M$ и K изоморфны, то мы и получаем требуемый изоморфизм $End_R M\cong D_n$. КД

I2. Строение простых колец. Мы имеем теперь все необходимое для завершения описания простых колец.

Теорема 3.I7 (вторая теорема Молина–Веддербарна). Пусть R – простое кольцо. Тогда R изоморфно кольцу D_n, где D – некоторое тело.

Д По доказанному ранее, R обладает единицей e и разлагается в прямую сумму попарно изоморфных минимальных левых идеалов:

$$R=M_1\dotplus M_2\dotplus\ldots\dotplus M_n,\ n\geq 1.$$

Если μ – эндоморфизм левого регулярного модуля ${}_R R$ и $e\mu=d$, то для любого $a\in R$ имеем:

$$a\mu=(ae)\mu=a(e\mu)=ad.$$

Таким образом, μ совпадает с правым умножением, производимым некоторым элементом $d\in R$. Обратно, каждое правое умножение $f(r)$, производимое элементом $r\in R$, является эндоморфизмом модуля ${}_R R$, так как для всех $a,b\in R$

$$(a+b)r=ar+br,\ (ab)r=a(br).$$

Так как $f(r_1r_2)=f(r_1)f(r_2)$, $f(r_1+r_2)=f(r_1)+f(r_2)$, то отображение f является эпиморфизмом кольца R на кольцо E всех эндоморфизмов модуля ${}_R R$. Так как из $r\neq 0$ следует, что $er=r\neq 0$, то $\operatorname{Ker} f=(0)$. Значит, $f: R\to E$ есть изоморфизм.

По теореме 3.I6, $E\cong D_n$, где $D=End_R M_1$ – тело. КД

Иногда оказываются полезными те дополнительные сведения, которые были получены в процессе доказательства теоремы 3.I7.

Теорема 3.I8. Пусть $M=Ra$ – минимальный левый идеал простого кольца R, порожденный идемпотентом a. И пусть n – число слагаемых в разложении кольца R в прямую сумму минимальных левых идеалов. Тогда $D=End_R Ra$ является телом, изоморфным телу aRa, а кольцо R изоморфно D_n.

Д По теореме 3.II, aRa является телом. Нам остается установить изоморфизм $D\cong aRa$. Если $d\in D$, то пусть $f(d)=ad\in Ra$. Тогда

$$af(d)=a(ad)=ad=f(d),$$

это означает, что $ad=f(d)\in aRa$. Легко видеть, что f является гомоморфизмом тела D в тело aRa. Если $f(d)=0$, то $(Ra)d=(0)$, откуда $ad=0$. Значит, $\operatorname{Ker} f=(0)$. Если $x\in aRa$, то отображение $d_1: rn\to rnx$, где $rn\in Ra$, принадлежит D, причем $f(d_1)=ad_1=ax=x$, так как x – единица aRa. Значит, $\operatorname{Im} f=aRa$, f – изоморфизм. КД

Следствие. Если R – кольцо с условием минимальности для левых идеалов, то $R/\operatorname{rad} R$ полупросто. Ненулевые полупростые кольца разлагаются в прямую сумму идеалов, являющихся простыми кольцами. Простые кольца исчерпываются полными матричными кольцами над телами.

ДОПОЛНЕНИЕ

Для удобства начинающего читателя мы приведем здесь необходимые начальные сведения из теории групп. О множествах и отображениях см. в [1], гл.I,§ 5. Если дано отображение $f: X \to Y$, то образ элемента $x \in X$ при этом отображении обозначают одним из следующих способов: $x^f, xf, fx, f(x)$. Если X_1 - подмножество множества X, то пишем $X_1 \subseteq X$; если же еще вдобавок $X_1 \neq X$, то пишем $X_1 \subset X$. Таким образом, символ $\subset$ мы употребляем только для обозначения строгого включения. Буквой $\mathbb{Z}$ мы обозначаем множество всех целых чисел.

I. Непустое множество G с бинарной алгебраической операцией $\cdot$ называется группой, если выполняются следующие условия:

а) операция ассоциативна, т.е. $(ab)c = a(bc)$ для любых $a, b, c \in G$;

б) G обладает таким элементом e, что $ae = a$ для любого $a \in G$;

в) для любого $a \in G$ существует такой элемент $a^{-1} \in G$, что $aa^{-1} = e$.

Группа обозначается символом $(G, \cdot)$ или чаще всего одной буквой G. Элемент e называется единичным или единицей группы G. Элемент a^{-1} называют обратным к a.

Группа G называется коммутативной (или абелевой), если $ab = ba$ для любых $a, b \in G$. Мощность группы G обозначается символом $|G|$. Если число элементов группы G конечно, то $|G|$ называют порядком группы G. Отметим простейшие следствия из определения группы.

I.1. Произведение любых $n \geqslant 3$ элементов группы не зависит от распределения скобок, указывающих на порядок, в котором должно выполняться умножение.

Доказательство проводится индукцией по n.

I.2. Для любого $a \in G$ имеем $a^{-1}a = e$, т.е. $(a^{-1})^{-1} = a$.

Д $a^{-1}a = a^{-1}ae = a^{-1}aa^{-1}(a^{-1})^{-1} = a^{-1}(aa^{-1})(a^{-1})^{-1} = a^{-1}(a^{-1})^{-1} = e$. КД

I.3. $ea = a$ для любого $a \in G$.

Д $ea = aa^{-1}a = a(a^{-1}a) = ae = a$. КД

I.4. e - единственная единица группы G.

Д Если $ae = ae' = a$ для любого $a \in G$, то по I.3 имеем: $ee' = e'e = e = e'$. КД

I.5. Если $ax = ay = e$, то $x = y$.

Д Согласно I.2, $xa = ya = e$. Поэтому $xay = (xa)y = x(ay) = ey = xe = y = x$. КД

Утверждение I.5 оправдывает обозначение a^{-1}, поскольку уравнение $ax = e$ имеет единственное решение $x = a^{-1} \in G$.

I.6. В группе G уравнение $ax = b$ имеет единственное решение, а именно $x = a^{-1}b$.

I.7. В группе G уравнение $ya = b$ имеет единственное решение, а именно $y = ba^{-1}$.

I.8. $(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1}$.

2. Положим $a^0 = e, a^1 = a, a^n = aa \dots a$ (n множителей, $n > 0$). Если m - отрицательное целое, то положим $a^m = (a^{-m})^{-1}$.

2.I. Равенства $a^m a^n = a^n a^m = a^{m+n}, (a^m)^n = a^{mn}$ выполняются при любых $m, n \in \mathbb{Z}$, $a \in G$.

Доказательство см. в [1], п.3 § 2 гл.4.

Непустое подмножество H из G называется подгруппой группы G, если для любых $h, k \in H$ имеет место $hk \in H$, $h^{-1} \in H$ (т.е. множество H образует группу). Подгруппа $\{e\}$ называется единичной и обозначается буквой E. Подгруппа группы G, отличная от G и E, называется нетривиальной.

Если $x \in G$, то $\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$ - циклическая подгруппа, порожденная элементом x. Если $\langle x \rangle = G$, то группа G называется циклической.

2.2. Пересечение $\bigcap_{i \in I} H_i$ любого семейства подгрупп $\{H_i \mid i \in I\}$ группы G также является подгруппой.

2.3. Непустое подмножество H из G тогда и только тогда является подгруппой, когда $hk^{-1} \in H$ для любых $h, k \in H$.

Утверждения 2.2 и 2.3 доказываются простой проверкой. Доказательство следующего утверждения см. в [1], п.3 § 2 гл.4.

2.4. Пусть $a \in G$. Если $a^i = a^j$ для некоторых целых $i, j \in \mathbb{Z}$, $i \neq j$, то $\langle a \rangle = \{a^0 = e, a, a^2, \dots, a^{n-1}\}$, где $n = |\langle a \rangle|$, причем равенство $a^m = e$, где $m \in \mathbb{Z}$, имеет место тогда и только в том случае, когда m делит n.

Если $a \in G$ и подгруппа $\langle a \rangle$ конечна, то говорят, что a – элемент конечного порядка $n = |\langle a \rangle|$. Если же подгруппа $\langle a \rangle$ бесконечна, то говорят, что a – элемент бесконечного порядка.

2.5. Всякая подгруппа циклической группы является циклической.

▲ Пусть $G = \langle a \rangle$, H – неединичная подгруппа из G. Если $a^i \in H$, то $(a^i)^{-1} = a^{-i} \in H$. Пусть m – наименьшее положительное целое такое, что $a^m \in H$. Тогда если $a^\alpha \in H$, $\alpha = mq + r$, $0 \le r < m$, то $a^\alpha = a^{mq} a^r$, $a^r = (a^{mq})^{-1} a^\alpha \in H$, откуда $r = 0$. КД

3. Некоторое непустое множество элементов группы G иногда называют ее частью. Условимся перемножать части M_1 и M_2 группы G следующим образом:

$$M_1 M_2 = \{m_1 m_2 \mid m_1 \in M_1, m_2 \in M_2\}.$$

Если $M_1 M_2 = M_2 M_1$, то части M_1 и M_2 называются перестановочными.

Если M – часть группы и $a \in G$, то $Ma = \{ma \mid m \in M\}$, $aM = \{am \mid m \in M\}$, $M^{-1} = \{m^{-1} \mid m \in M\}$.

3.1. $Ga = aG = G$ для любого $a \in G$.

▲ Вытекает из I.6 и I.7. КД

Пусть H – подгруппа группы G, $x \in G$. Тогда Hx называется левым смежным классом, а xH – правым смежным классом группы G по подгруппе H.

3.2. Левые и правые смежные классы группы G по подгруппе H обладают следующими свойствами:

а) $|Hx| = |xH| = |H|$;

б) если $y \in Hx$, то $Hx = Hy$; если $z \in xH$, то $zH = xH$;

в) $(Hx)^{-1} = x^{-1}H$, $(xH)^{-1} = Hx^{-1}$.

Доказательство – проверкой. Из 3.2 б) вытекает, что любые два левых (правых) смежных класса по H либо совпадают, либо не имеют общих элементов. Из 3.2 выводим справедливость следующих двух утверждений.

3.3. Пусть $\{Hx_i \mid i \in I\}$ – множество всех различных левых смежных классов, а $\{y_j H \mid j \in J\}$ – множество всех различных правых смежных классов группы G по подгруппе H. Тогда:

а) $G = \bigcup_{i \in I} Hx_i$, причем $Hx_{i_1} \cap Hx_{i_2} = \varnothing$ при $i_1 \neq i_2$;

б) $G = \bigcup_{j \in J} y_j H$, причем $y_{j_1} H \cap y_{j_2} H = \varnothing$ при $j_1 \neq j_2$;

в) $|I| = |J|$.

Мощность $|I|$ из 3.3 называется индексом подгруппы H в группе G и обозначается через $|G:H|$.

3.4. Теорема Лагранжа. Если H – подгруппа конечной группы G, то $|G| = |H| \cdot |G:H|$.

4. Введем обозначение: если $M \subseteq G$, $x \in G$, то $M^x = x^{-1}Mx$. На множестве всех частей группы G введем отношение $\sim_G$, полагая $M \sim_G H$ тогда и только тогда, когда $M^x = H$ для некоторого $x \in G$. Если $M \sim_G H$, то говорят, что части M и H сопряжены в G. Тогда $\sim_G$ есть отношение эквивалентности. Отношением $\sim_G$ множество всех элементов группы G разбивается на классы сопряженных элементов, а множество всех подгрупп группы G – на классы сопряженных подгрупп.

Часть M группы G называется нормальной (или инвариантной), если она совпадает со всеми своими сопряженными. Другими словами, часть M называется нормальной в G, если выполняется одно из следующих равносильных условий: 1) $M^x = M$ для любого $x \in G$; 2) $Mx = xM$ для любого $x \in G$; 3) $m^x \in M$ для любого $m \in M$ и любого $x \in G$. Запись $H \triangleleft G$ означает, что H есть нормальная подгруппа группы G.

Классы сопряженных элементов являются нормальными частями группы. Действительно, если $a \in G$, $C = \{a^x \mid x \in G\}$, то ввиду $Gy = G$ имеем $C^y = \{a^{xy} \mid x \in G\} = C$.

5. Пусть дана группа G с единицей e и группа Γ с единицей ε. Отображение $f: G \to \Gamma$ называется гомоморфизмом группы G в группу Γ, если $(xy)^f = x^f y^f$ для любых $x, y \in G$. Нетрудно убедиться в том, что при гомоморфизме $f: G \to \Gamma$ имеют место $e^f = \varepsilon$, $(a^{-1})^f = (a^f)^{-1}$ для любого $a \in G$. Если $M \subseteq G$, то $M^f = \{m^f \mid m \in M\}$ – образ части M при гомоморфизме f. Часть $G^f = \mathrm{Im} f$ называется образом, а $\mathrm{Ker} f = \{x \in G \mid x^f = \varepsilon\}$ – ядром гомоморфизма f.

5.I. Если f – гомоморфизм группы G в группу Γ, то G^f – подгруппа группы Γ, а $\mathrm{Ker} f$ – нормальная подгруппа группы G.

Доказательство – проверкой.

Если $H \lhd G$, то множество $G/H=\{xH \mid x\in G\}$ с операцией умножения смежных классов $(xH)(yH)=xyH$ является группой. Группа G/H называется фактор-группой группы G по H.

Очевидно следующее утверждение.

5.2. Если $H \lhd G$, то отображение $x \mapsto xH, x\in G$ является гомоморфизмом группы G в G/H. Этот гомоморфизм называется естественным, его ядро совпадает с H.

Гомоморфизм $f: G \to \Gamma$ называется:

а) изоморфизмом, если отображение f взаимно однозначно (в этом случае группы G и Γ называют изоморфными и пишут $G \simeq \Gamma$);

б) эпиморфизмом (или гомоморфизмом на Γ), если $\mathrm{Im} f=\Gamma$;

в) мономорфизмом, если $\mathrm{Ker} f=E$.

5.3. Если дан гомоморфизм $f: G \to \Gamma$, то $G/\mathrm{Ker} f \simeq \mathrm{Im} f$.

Д Пусть $\varphi: x\mathrm{Ker} f \mapsto x^f$. Проверка показывает, что φ – искомый изоморфизм группы $G/\mathrm{Ker} f$ на $\mathrm{Im} f$. КД

5.4. Теорема Кэли. Всякая группа изоморфна группе взаимно однозначных отображений некоторого множества на себя.

Доказательство см. в [2], с.I07.

5.5. Любые две бесконечные циклические группы изоморфны. Любые две конечные циклические группы одинакового порядка изоморфны.

Д Если $\langle a\rangle$ и $\langle b\rangle$ – циклические группы одинаковой мощности, то $\varphi: a^i \mapsto b^i$, $i\in\mathbb{Z}$, есть искомый изоморфизм. КД

6. Если A – группа с операцией, обозначенной знаком $+$ (сложение), то такая группа называется аддитивной. В этом случае изменяют терминологию и вместо единицы и обратного элемента говорят о нуле 0 и противоположном элементе $-a$. Нулевая подгруппа аддитивной группы A обозначается буквой 0.

ЛИТЕРАТУРА

I. КОСТРИКИН А.И. Введение в алгебру. – М.: Наука, 1977.
2. КАРГАПОЛОВ М.И., МЕРЗЛЯКОВ Ю.И. Основ. теории групп. М.: Наука, 1977.
3. ВАН ДЕР ВАРДЕН Б.Л. Алгебра. – М.: Наука, 1979.
4. КУРОШ А.Г. Лекции по общей алгебре. – М.: Наука, 1962.
5. КУРОШ А.Г. Теория групп. – М.: Наука, 1967.
6. ЕРШОВ Ю.Л., ПАЛЮТИН Е.А. Математическая логика. – М. Наука, 1979.
7. ФЕЙС К. Алгебра: кольца, модули и категории, т.I,2. М.: Мир, 1977, 1979.
8. ДЖЕКОБСОН Н. Строение колец. – М.: ИЛ, 1961.
9. АНДРУНАКИЕВИЧ В.А., РЯБУХИН Ю.М. Радикалы алгебр и структурная теория. – М.: Наука, 1979.

ОГЛАВЛЕНИЕ

Леонид Александрович Неметков

Классические факторизации групп и колец

(Учебное пособие)

Редактор Е.Ф.Зайцева

Подписано к печати 25. I2. 1979 г. Формат 60x90 1/16. Бумага писчая № I. Печать офсетная. Усл.п.л. 3,7. Уч.-изд.л. 3,4. Тираж 500. Заказ № 352 Цена I2 к.

Отпечатано на ротапринте ГГУ, г.Гомель, ул.Советская, 104