ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное
учреждение высшего образования
“ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ ИМПЕРАТОРА АЛЕКСАНДРА I”

Кафедра «Высшая математика»

Е.А. Благовещенская

Конспект лекций

по дисциплине

«АЛГЕБРА И ГЕОМЕТРИЯ» (Б1.Б.13)

для специальности
10.05.03 «Информационная безопасность автоматизированных систем»

по специализации
«*Безопасность автоматизированных систем на железнодорожном транспорте*»

Форма обучения – очная

РАЗДЕЛ 7. ТЕОРИЯ ГРУПП И КОЛЕЦ

Санкт-Петербург 2023

Лекция 15. Классы смежности по подгруппе. Гомоморфизм групп. Циклические группы. Разложение абелевых групп.

Определение 3.1. Пусть H – подгруппа группы G. Элементы $g_1, g_2 \in G$ называются *эквивалентными слева (справа)* относительно подгруппы H, если $\exists h \in H: \ g_1 = h * g_2$ ($g_1 = g_2 * h$).

Определение. *Гомоморфизм групп* $(G, *)$ и $(L, \circ)$ — отображение $\varphi\colon G \to L$, сохраняющее операцию: $\forall\, a, b \in$ $\in G$ имеем $\varphi(a * b) = \varphi(a) \circ \varphi(b)$.

Пусть e — единица G, а e' — единица в L. Покажем, что $\varphi(e) = e'$. В самом деле, $\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$, значит, $\varphi(e)$ — нейтральный элемент в L. Покажем, что $\varphi(a^{-1}) = \varphi(a)^{-1}$. В самом деле, рассмотрим $e' = \varphi(e) =$ $= \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$, т. е. $\varphi(a^{-1})$ — обратный элемент по отношению к $\varphi(a)$.

Определение. Биективный гомоморфизм $\varphi\colon G \to L$ называется *изоморфизмом* групп. При этом говорят, что группы G и L *изоморфны*, и пишут $G \cong L$. Изоморфизм группы на себя называется *автоморфизмом*.

Определение. *Ядро* гомоморфизма φ — множество $\operatorname{Ker}\varphi := \{g \in G\colon \varphi(g) = e'\}$. *Образ* гомоморфизма — множество $\operatorname{Im}\varphi := \{x \in L\colon \exists\, g \in G\colon \varphi(g) = x\}$.

Утверждение 1.2. *$\operatorname{Ker}\varphi$ является подгруппой в G, $\operatorname{Im}\varphi$ является подгруппой в L.*

□ Пусть $g, h \in \operatorname{Ker}\varphi$. Тогда $\varphi(gh) = \varphi(g)\varphi(h) = e'e' = e' \Rightarrow gh \in \operatorname{Ker}\varphi$. Очевидно, $e \in \operatorname{Ker}\varphi$. Кроме того, если $g \in \operatorname{Ker}\varphi$, то $\varphi(g^{-1}) = \varphi(g)^{-1} = e'^{-1} = e' \Rightarrow g^{-1} \in \operatorname{Ker}\varphi$.

Пусть $x, y \in \operatorname{Im}\varphi$, тогда $\exists\, g, h \in G\colon x = \varphi(g), y = \varphi(h)$. Тогда $x^{-1}y = \varphi(g)^{-1}\varphi(h) = \varphi(g^{-1}h) \in \operatorname{Im}\varphi$. Используя эквивалентное определение подгруппы, получаем требуемое утверждение. ■

Определение. Инъективный гомоморфизм называется *вложением* группы G в группу L и обозначается $\varphi\colon G \hookrightarrow L$. В этом случае $G \cong \operatorname{Im}\varphi$.

Заметим, что гомоморфизм инъективен $\Leftrightarrow \operatorname{Ker}\varphi = \{e\}$. В самом деле, пусть $\operatorname{Ker}\varphi = \{e\}$. Тогда $\varphi(a) = \varphi(b) \Leftrightarrow$ $\Leftrightarrow \varphi(a^{-1}b) = e' \Leftrightarrow a^{-1}b = e \Leftrightarrow a = b$. Обратно, пусть гомоморфизм инъективен. Тогда $a \in \operatorname{Ker}\varphi \Leftrightarrow \varphi(a) = e'$. Но $\varphi(e) = e'$, и в силу инъективности $a = e$. Значит, $\operatorname{Ker}\varphi$ содержит только e.

Пусть $\varphi\colon G \to L$ — гомоморфизм, и H — подгруппа в G. Покажем, что $K = \varphi(H)$ — подгруппа в L. Рассмотрим $x, y \in K$. Тогда $\exists\, a, b \in H\colon x = \varphi(a), y = \varphi(b)$. Тогда $xy = \varphi(a)\varphi(b) = \varphi(ab)$, значит, $xy \in K$. Поскольку $e \in H$, а $\varphi(e) = e'$, получаем, что $e' \in K$. Покажем, что $x^{-1} \in K$. Действительно, $x^{-1} = \varphi(a^{-1}) \in K$, поскольку $a^{-1} \in H$.

Определение. Сюръективный гомоморфизм называется *эпиморфизмом*.

Пусть $\varphi\colon G \to L$ — эпиморфизм, и K — подгруппа в L. Тогда $H = \varphi^{-1}(K)$ — подгруппа в G. В самом деле, пусть $x, y \in H$, тогда $\varphi(x), \varphi(y) \in K$. Рассмотрим $\varphi(x^{-1}y) = \varphi(x)^{-1}\varphi(y) \in K$. Следовательно, $x^{-1}y \in H$, значит, H — подгруппа.

Пример 2.1.

1° Пусть $n \in \mathbb{N}$. Рассмотрим $\varphi\colon (\mathbb{Z}, +) \to \mathbb{C}^*$, определённый по правилу $\varphi\colon k \mapsto \varepsilon_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$. Тогда φ — гомоморфизм. Очевидно, $\operatorname{Ker}\varphi = n\mathbb{Z}$.

2° *Левый сдвиг.* Пусть G — группа. Фиксируем $g \in G$, и рассмотрим отображение $L_g\colon G \to G$, определённое по правилу $L_g\colon x \mapsto gx$. Покажем, что $L_g \in \mathcal{S}_G$, где $\mathcal{S}_G$ — группа подстановок множества G. Действительно, оно сюръективно: $L_g(g^{-1}x) = g(g^{-1}x) = x$. Кроме того, $L_g(x) = L_g(y) \Leftrightarrow gx = gy \Leftrightarrow x = y$. Значит, это инъекция. Теперь рассмотрим множество всех левых сдвигов $L_G := \{L_g\colon g \in G\}$. Это подгруппа в $\mathcal{S}_G$, поскольку произведение сдвигов на элементы g_1 и g_2 есть левый сдвиг на элемент g_1g_2, нейтральным элементом в L_G будет левый сдвиг на $e \in G$, обратным к сдвигу на g — сдвиг на g^{-1}. Таким образом, $L_G \subset \mathcal{S}_G$.

Теорема 1.3 (Кэли). *Пусть G — группа. Тогда $\exists$ инъективный гомоморфизм $G \hookrightarrow \mathcal{S}_G$.*

□ Рассмотрим $\varphi\colon G \to \mathcal{S}_G$ по правилу $\varphi\colon g \mapsto L_g$. Тогда φ — искомый гомоморфизм, ибо $\varphi(g_1g_2) = L_{g_1g_2} =$ $= L_{g_1}L_{g_2} = \varphi(g_1)\varphi(g_2)$, а его инъективность очевидна. ■

Лекция 16. Кольца. Основные свойства колец. Кольцо многочленов над полем комплексных и вещественных чисел.

Определение 1. *Бинарной операцией* на множестве X называется отображение $f: X \times X \to X$, которое сопоставляет паре элементов (x_1, x_2) множества X элемент того же множества, т.е. $f(x_1, x_2) \in X$.

Обозначение для произвольной операции: $f(x_1, x_2) = x_1 * x_2$.

Примерами операций являются сложение (+) и умножение ($\cdot$) на множестве вещественных чисел $\mathbf{R}$.

Определение 2. Множество G называется *группой,* если на нем задана операция $*$ со следующими свойствами:

1. $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$ – ассоциативность;
2. $\exists e \in G: \quad \forall g \in G \quad e * g = g * e = g$ – наличие единичного элемента;
3. $\forall g \in G \quad \exists g^{-1} \in G: \quad g * g^{-1} = g^{-1} * g = e$ – наличие обратного элемента.

Определение 3. Группа G называется *коммутативной* или *абелевой*, если операция $*$ в ней коммутативна, т.е. $g_1 * g_2 = g_2 * g_1$.

В качестве примера можно рассмотреть множество целых чисел $\mathbf{Z}$. Относительно операции сложения множество $\mathbf{Z}$ будет являться группой (единичным элементом будет 0, а обратным – противоположное число), кроме того, эта группа будет абелевой.

С другой стороны, множество $\mathbf{Z}$ относительно операции умножения не будет группой (не все элементы имеют обратный).

Определение 4. Множество $\mathbf{K}$ называется *кольцом,* если на этом множестве определены *две* операции: *сложения* и *умножения*. Относительно операции сложения множество $\mathbf{K}$ является *абелевой группой*, а относительно умножения множество $\mathbf{K} \setminus \{0\}$ является *полугруппой*. Умножение и сложение связаны между собой законом дистрибутивности:

1. $(a+b) \cdot c = a \cdot c + b \cdot c$;
2. $a \cdot (b+c) = a \cdot b + a \cdot c$.

Определение5. Кольцо $\mathbf{K}$ называется *коммутативным*, если операция умножения коммутативна. Если полугруппа $\mathbf{K} \setminus \{0\}$ относительно умножения имеет единицу, то кольцо называется *кольцом с единицей*.

Примерами колец могут служить множества рациональных $\mathbf{Q}$ и комплексных чисел $\mathbf{C}$. Причем оба эти кольца являются коммутативными с единицей, т.к. операция умножения коммутативна, а единицей будет служить 1.

Кольцом является множество *неособых квадратных матриц* (т.е. матриц, определитель которых отличен от нуля). В качестве единицы относительно сложения будет нулевая матрица, а единицей относительно умножения – единичная матрица. Но это кольцо не будет коммутативным, поскольку операция умножения матриц коммутативностью не обладает.

Определение 6. Кольцо $\mathbf{K}$ называется *телом*, если относительно операции умножения в $\mathbf{K}$ каждый элемент обратим.

Определение 7.Коммутативное тело называется *полем,* обозначение*:* $\mathbf{F}$

Примерами полей являются множества вещественных– $\mathbf{R}$ и комплексных– $\mathbf{C}$ чисел.

Определение 8. Пусть K – некоторое коммутативное кольцо с единицей, и пусть x – буква, посторонняя для кольца K. *Одночленом* степени m от буквы x с коэффициентом из K называется выражение ax^m, где $a \in K$, m – целое неотрицательное число.

Будем считать, что $ax^0 = a$. Таким образом, элементы кольца K являются одночленами частного вида.

Определение 9. Формальное выражение, состоящее из нескольких одночленов, соединенных знаком +, называется *многочленом* или *полиномом* от x с коэффициентами из K.

Предполагается, что порядок следования одночленов безразличен, подобные одночлены можно соединять, а также вставлять и выбрасывать одночлены с нулевыми коэффициентами. Без нарушения общности можно считать полином записанным в канонической форме $a_0x^n + a_1x^{n-1}+...+a_n$ (т.е. в порядке убывания степеней) или в порядке возрастания степеней $c_0 + c_1x+...+c_nx^n$.

Определение 10. Два полинома считаются *равными*, если они составлены в канонической записи из одинаковых одночленов, т.е. $a_0x^n + a_1x^{n-1}+...+a_n = b_0x^n + b_1x^{n-1}+...+b_n$ в том и только в том случае, если $a_i = b_i,\ i = 0,\ 1,\ \ldots,\ n$.

Определение 11. *Суммой* двух полиномов называется полином, получающийся посредством объединения одночленов, составляющих слагаемые. Разумеется, после объединения следует привести подобные члены. Таким образом, $(a_0x^n + a_1x^{n-1}+...+a_n) + (b_0x^n + b_1x^{n-1}+...+b_n) = (a_0 + b_0)x^n + (a_1 + b_1)x^{n-1}+...+(a_n + b_n) = c_0x^n + c_1x^{n-1}+...+c_n$, где $c_i = a_i + b_i,\ i = 0,\ 1,\ \ldots,\ n$.

Замечание: Если многочлены $f(x)$ и $g(x)$ имеют разное число одночленов, то, подписав необходимое число одночленов с нулевыми коэффициентами к одному из них, в котором число одночленов меньше, можно добиться их равенства в обоих многочленах. Поэтому складывать можно многочлены с разным числом одночленов.

Заметим, что операция сложения многочленов обладает такими же свойствами, что и операция сложения элементов кольца K, т.е. ассоциативна, коммутативна; полином, все коэффициенты которого нули, является нейтральным элементом сложения полиномов; для каждого полинома существует ему противоположный, противоположный к полиному $a_0x^n + a_1x^{n-1}+...+a_n$ является полином $-a_0x^n - a_1x^{n-1}-...-a_n$. Итак, множество полиномов с операцией сложения образует коммутативную группу.

Определение 12. *Произведением* двух полиномов называется полином, составленный из произведений всех членов первого сомножителя на все члены второго.

Таким образом, $(a_0x^n + a_1x^{n-1} + ... + a_n)(\mathrm{b}_0\, x^m + b_1x^{m-1} + ... + b_m) =$ $= -c_0x^{n+m} + c_1x^{n+m-1} + ... + c_{n+m}$, где $c_k = \sum_{i+j=k} a_i b_j$.

Умножение многочленов ассоциативно, коммутативно и дистрибутивно относительно сложения, роль единицы при умножении многочленов играет многочлен $f(x) \equiv 1$ (где 1 – единица кольца *K*). Таким образом, множество полиномов от буквы *x* с коэффициентами из кольца составляет кольцо по отношению к выше определенным операциям сложения и умножения полиномов. Кольцо это коммутативно оно называется *кольцом полиномов* от буквы *x* над кольцом *K* и обозначается *K*[*x*].

Пусть $f(x) = a_0x^n + a_1x^{n-1} + ... + a_n$, причем $a_0 \neq 0$. Одночлен a_0x^n называется *высшим* (*старшим*) *членом* полинома *f*(*x*) и показатель *n* называется *степенью f*(*x*) и обозначается deg *f*. Нулевой полином не имеет высшего члена в смысле данного определения и считается, что он равен нулю. Коэффициент a_n называется *свободным членом*. Многочлен, старший коэффициент которого равен единице, называется *нормированным*.

Простейшие свойства степени многочлена:

1. $\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$;
2. $\deg f(x)g(x) \leq \deg f(x) + \deg g(x)$.

Далее *будем рассматривать только многочлены с коэффициентами из области целостности K* (кольцо без делителей нуля называют областью целостности), т.е. из кольца *K*, в котором произведение двух элементов может равняться нулю, если только один из сомножителей равен нулю. Это всегда будет подразумеваться, даже если не будет оговорено специально.

При произведении многочленов $f(x) = a_0x^n + a_1x^{n-1} + ... + a_n$ степени *n* и $g(x) = b_0x^m + b_1x^{m-1} + ... + b_m$ степени *m* старший член равен a_0b_0 (это коэффициент при x^{n+m}). Так как в кольце нет делителей нуля, то $a_0b_0 \neq 0$ и, значит, $f(x)g(x) \neq 0$. Следовательно, $\deg f(x)g(x) = \deg f(x) + \deg g(x)$.

Итак, произведение двух ненулевых многочленов – ненулевой многочлен, поэтому справедлива следующая теорема:

Теорема 1. *Кольцо многочленов над областью целостности само является областью целостности.*

Данное нами алгебраическое определение многочлена не содержит никакого упоминания о функциях. Тем не менее, с каждым многочленом над областью целостности *K* можно естественным образом связать функцию, которая определена на *K* и принимает значения в *K*.

Пусть $f(x) = a_0x^n + a_1x^{n-1} + ... + a_n$ – многочлен с коэффициентами из *K*. Для любого $x_0 \in K$ положим $f(x_0) = a_0x_0^n + a_1x_0^{n-1} + ... + a_0$, где выражение в правой части понимается как результат операций в кольце *K*. Получаемый при этом элемент

$f(x_0) \in K$ называется значением многочлена $f(x)$ в точке x_0. Таким образом, каждому элементу x_0 кольца K сопоставляется элемент $f(x_0)$ того же кольца и тем самым определяется функция на K со значениями в K.

Вообще говоря, соответствие между многочленами и определяемыми ими функциями не является взаимно однозначным. Однако, если кольцо K бесконечно, то различным многочленам из кольца $K[x]$ всегда соответствуют различные функции.