3-й модуль

1 Определения

1.1 Какие бинарные операции называются ассоциативными, а какие коммутативными?

Определение. Пусть X – множество с заданной на нём бинарной операцией $*$. $*$ – ассоциативна, если: $\forall a, b, c \in X \;\; a * (b * c) = (a * b) * c$.

Бинарная операция $*$ – коммутативна, если: $\forall a, b \in X \;\; a * b = b * a$

1.2 Дайте определения полугруппы и моноида. Приведите примеры.

Определение. Множество X с заданной на нём бинарной ассоциативной операцией называется полугруппой.

Определение. Полугруппа, в которой есть нейтральный элемент – моноид.

Пример полугруппы. $(\mathbb{N} \setminus \{1\}, \cdot)$, $\cdot$ – умножение натуральных чисел.
Пример моноида. $(\mathbb{N}, \cdot)$

1.3 Сформулируйте определение группы. Приведите пример.

Определение (эквивалентное)**.** Множество G с корректно определённой на нём бинарной операцией $*$ называется группой, если:

1) операция ассоциативна: $\forall x, y, z \in G \; x * (y * z) = (x * y) * z$
2) $\exists e \in G \; \forall x \in G : x * e = e * x = x$
3) $\forall x \in G \; \exists x^{-1} \in G : x * x^{-1} = x^{-1} * x = e$

Пример. $(\mathbb{Z}, +)$

1.4 Что такое симметрическая группа? Укажите число элементов в ней.

Определение. Симметрическая группа S_n – множество всех подстановок длинны n: $\sigma = \begin{pmatrix} 1 & \dots & n \\ i_1 & \dots & i_n \end{pmatrix}$ с операцией композиции. Число элементов в S_n равно числу перестановок: $n!$

1.5 Что такое общая линейная и специальная линейная группы?

Определение. Общая линейная группа – множество всех невырожденных матриц A с операцией матричного умножения: $GL_n(\mathbb{R})$ (n – размер матрицы).

Определение. Специальная линейная группа – $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid \det A = 1\}$, $SL_n(\mathbb{R}) \subset GL_n(\mathbb{R})$. Это множество замкнуто относительно умножения и взятия обратного.

1.6 Сформулируйте определение абелевой группы. Приведите пример.

Определение. Группа с коммутативной операцией называется абелевой.

Пример. $(\mathbb{Z}, +)$

1.7 Дайте определение подгруппы. Приведите пример группы и её подгруппы.

Определение. Подмножество $H \subseteq G$ называется подгруппой в G, если:
1) $e \in H$
2) Если $h_1, h_2 \in H \Rightarrow h_1 \cdot h_2 \in H$, т.е. множество H замкнуто относительно умножения.
3) Если $h \in H \Rightarrow h^{-1} \in H$, т.е. H замкнуто относительно взятия обратного.

Пример. Специальная линейная группа: $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid \det A = 1\}$, $SL_n(\mathbb{R}) \subset GL_n(\mathbb{R})$. Это множество замкнуто относительно умножения и взятия обратного.

1.8 Дайте определение гомоморфизма групп. Приведите пример.

Определение. Пусть даны две группы: $(G_1, *)$ и $(G_2, \circ)$. Тогда отображение $f : G_1 \to G_2$ называется гомоморфизмом, если выполняется следующее условие: $\forall a, b \in G_1 \ f(a * b) = f(a) \circ f(b)$.

Пример. $G_1 = (\mathbb{R}_+, \cdot)$, $G_2 = (\mathbb{R}, +)$ и гомоморфизмом $f = \ln x$. Является гомоморфизмом по определению $\forall a, b \in G_1 \ \ln(a \cdot b) = \ln a + \ln b$.

1.9 Дайте определение изоморфизма групп. Приведите пример.

Определение. Биективный гомоморфизм называется изоморфизмом.

Пример. $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$ и изоморфизмом $f = e^x$.

1.10 Дайте определение порядка элемента.

Определение. Пусть q – наименьшее натуральное ($\neq 0$) число, для которого $a^q = e$, где $a \in G$, оно называется порядком элемента. Если такого числа не существует, то говорят об элементе бесконечного порядка.

1.11 Сформулируйте определение циклической группы. Приведите пример.

Определение. Пусть g – элемент G. Если любой элемент $g \in G$ имеет вид $g = a^n$, где $a \in G$, то G называют циклической группой.

1.12 Сколько существует, с точностью до изоморфизма, циклических групп данного порядка?

Утверждение. Все циклические группы одного порядка изоморфны.

Утверждение. Для каждого числа существует единственная (с точностью до изоморфизма) циклическая группа такого порядка. Также существует ровно одна бесконечная циклическая группа.

1.13 Что такое ядро гомоморфизма групп? Приведите пример.

Определение. Ядром гомоморфизма $f : G \to F$ называется множество элементов группы G, которые переходят в e_F (нейтральный элемент во второй группе).

$$\operatorname{Ker} f = \{g \in G \mid f(g) = e_F\}$$

Пример. $\varphi : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$, $\varphi(x) = x \mod 3$, $\operatorname{Ker}\varphi = \{x \in \mathbb{Z} \mid x \,\vdots\, 3\}$

Пример. $\det : GL_n(\mathbb{R}) \to \mathbb{R}^* = \{\mathbb{R} \setminus \{0\}, \cdot\}$, $\operatorname{Ker}\det = SL_n(\mathbb{R}) = \{A \mid \det A = 1\}$

1.14 Сформулируйте утверждение о том, какими могут быть подгруппы группы целых чисел по сложению.

Утверждение. Любая подгруппа в $(\mathbb{Z}, +)$ имеет вид $k\mathbb{Z}$ (числа, кратные k) для $k \in \mathbb{N} \cup \{0\}$.

1.15 Дайте определение левого смежного класса по некоторой подгруппе.

Определение. Пусть G – группа и H – её подгруппа. Пусть фиксирован $g \in G$. Левым смежным классом элемента g по подгруппе H называется множество $gH = \{g \cdot h | h \in H\}$ (а правым смежным класс: $Hg = \{h \cdot g \mid h \in H\}$).

1.16 Дайте определение нормальной подгруппы.

Определение. Подгруппа H группы G называется нормальной, если $gH = Hg$, $\forall g \in G$.

1.17 Что такое индекс подгруппы?

Определение. Индексом подгруппы H в группе G называется количество левых смежных классов G по H.

1.18 Сформулируйте теорему Лагранжа.

Теорема (Лагранжа)**.** Пусть G – конечная группа и $H \subseteq G$ – её подгруппа. Тогда

$$|G| = |H| \cdot [G : H]$$

1.19 Сформулируйте три следствия из теоремы Лагранжа.

Следствие. Пусть G – конечная группа и $g \in G$. Тогда $\operatorname{ord} g$ делит $|G|$.

Следствие. Пусть G – конечная группа и $g \in G$. Тогда

$$g^{|G|} = e$$

Следствие (Малая теорема Ферма)**.** Пусть $\bar{a}$ – ненулевой вычет по простому модулю p. Тогда

$$\bar{a}^{p-1} = \bar{1} \text{ (или } \bar{a}^p = \bar{a})$$

1.20 Сформулируйте критерий нормальности подгруппы, использующий сопряжение.

Утверждение. Пусть $H \subseteq G$. Тогда три условия эквивалентны:

(1) H нормальная
(2) $gHg^{-1} \subseteq H, \forall g \in G$
(3) $\forall g \in G\ gHg^{-1} = H$

1.21 Сформулируйте определение простой группы.

Определение. Группа называется простой, если она не имеет собственных (т.е. отличных от единичной и самой группы) нормальных групп.

1.22 Дайте определение факторгруппы.

Определение. Пусть H – нормальная подгруппа в G. G/H – множество левых смежных классов по H с операцией умножения $(g_1H)(g_2H) = g_1g_2H$ называется факторгруппой.

1.23 Что такое естественный гомоморфизм?

Определение. Отображение $\varepsilon : G \to G/H$ называется естественным гомоморфизмом.

$\varepsilon : a \longmapsto aH$, где $a \in G$, aH – смежный класс, содержащий a

1.24 Сформулируйте критерий нормальности подгруппы, использующий понятие ядра гомоморфизма.

Утверждение. H – нормальная подгруппа в $G \Leftrightarrow H = \operatorname{Ker} f$, f – гомоморфизм.

1.25 Сформулируйте теорему о гомоморфизме групп. Приведите пример.

Теорема (о гомоморфизме)**.** Пусть $f : G \to F$ – гомоморфизм групп. Тогда $\operatorname{Im} f$ изоморфен факторгруппе $G/\operatorname{Ker} f$, т.е. $G/\operatorname{Ker} f \cong \operatorname{Im} f$, где $\operatorname{Im} f = \{a \in F \mid \exists g \in G : f(g) = a\}$ – образ f.

Пример:

$$f : GL_n(\mathbb{R}) \xrightarrow{\det A} \mathbb{R}^* = \{\mathbb{R} \setminus \{0\}, \cdot\}$$

$$\operatorname{Ker}\det = SL_n(\mathbb{R}) = \{A \mid \det A = 1\} \Rightarrow GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \underbrace{\mathbb{R}^*}_{\operatorname{Im}\det}$$

1.26 Что такое прямое произведение групп?

Определение. Прямым произведением двух групп G_1 и G_2 называется их прямое (декартовое) произведение как множеств с покомпонентным умножением:

$$(x_1, y_1) \circ (x_2, y_2) = (x_1 * x_2, y_1 \star y_2)$$

$*$ – произведение в G_1, $\star$ – произведение в G_2

1.27 Сформулируйте определение автоморфизма и внутреннего автоморфизма.

Определение. Автоморфизм – это изоморфизм из G в G.

Определение. Внутренним автоморфизмом называют отображение $I_n : g \mapsto aga^{-1}$

1.28 Что такое центр группы? Приведите пример.

Определение. Центр группы G – это множество $Z(G) = \{a \in G \mid ab = ba \, \forall b \in G\}$, т.е. множество элементов, которые коммутируют со всеми.

Пример. Центр группы кватернионов $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ равен $\{1, -1\}$.

1.29 Что можно сказать про факторгруппу группы по её центру?

$G/Z(G) \cong I_{nn}(G)$, $I_{nn}(G)$ – внутренние автоморфизмы.

1.30 Сформулируйте теорему Кэли.

Теорема (Кэли)**.** Любая конечная группа порядка n изоморфна некоторой подгруппе группы S_n.

1.31 Дайте определение кольца.

Определение. Пусть $K \neq \varnothing$ – множество на котором заданы две бинарные операции: $+$ и $\cdot$, что:

1) $(K, +)$ – абелева группа.
2) $(K, \cdot)$ – полугруппа.
3) Умножение дистрибутивно по сложению: $\forall a, b, c$

$$(a + b)c = ac + bc$$
$$c(a + b) = ca + cb$$

1.32 Что такое коммутативное кольцо? Приведите примеры коммутативного и некоммутативного колец.

Определение. Если $\forall x, y \in K \; xy = yx$ (т.е. умножение коммутативно), то кольцо $(K, +, \cdot)$ называется коммутативным.

Пример. $(\mathbb{Z}, +, \cdot)$ – коммутативное кольцо.

Пример. $(M_n(\mathbb{R}), +, \cdot)$ – некоммутативное кольцо.

1.33 Дайте определение делителей нуля.

Определение. Если $ab = 0$ при $a \neq 0$ и $b \neq 0$ в кольце K, то a называется левым, b – правым делителем нуля.

1.34 Какие элементы кольца называются обратимыми?

Определение. Элемент коммутативного кольца с "1" называется обратимым (по умножению), если существует $a^{-1} : aa^{-1} = a^{-1}a = 1$.

1.35 Дайте определение поля. Приведите три примера.

Определение. Поле P – это коммутативное кольцо с единицей ($1 \neq 0$), в котором каждый элемент $a \neq 0$ обратим.

Пример. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

1.36 Дайте определение подполя. Привести пример пары: поле и его подполе.

Определение. Подполе – подмножество поля, которое само является полем относительно тех же операций.

Пример. $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

Пример. $\mathbb{Z}_p$, где p – простое, тоже является полем.

1.37 Дайте определение характеристики поля. Привести примеры: поля конечной положительной характеристики и поля нулевой характеристики.

Определение. Пусть P – поле. Характеристикой поля называется такое наименьшее $q \in \mathbb{N}$, что $\underbrace{1 + 1 + \ldots + 1}_{q} = 0$. Если такого q нет, то характеристика равна 0.

Пример. $\operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = \operatorname{char} \mathbb{Q} = 0$

Пример. $\operatorname{char} \mathbb{Z}_p = p$

1.38 Сформулируйте утверждение о том, каким будет простое подполе в зависимости от характеристики.

Утверждение. Пусть P – поле, а P_0 – его простое подполе. Тогда:

1) Если характеристика поля $\operatorname{char} P = p > 0$, то $P_0 \cong \mathbb{Z}_p$
2) Если $\operatorname{char} P = 0$, то $P_0 \cong \mathbb{Q}$.

1.39 Дайте определение идеала. Что такое главный идеал?

Определение. Подмножество I кольца K называется (двусторонним) идеалом, если оно:

1) является подгруппой $(K, +)$ по сложению
2) $\forall a \in I \, \forall r \in K \; ra \in I$ и $ar \in I$

Определение. Идеал I называется главным, если $\exists a \in K : I = \{ra \mid r \in K\}$. Говорят, что идеал I порождён a.

1.40 Сформулируйте определение гомоморфизма колец.

Определение. $\varphi : K_1 \to K_2$ – гомоморфизм колец, если $\forall a, b \in K_1$:

1) $\varphi(a + b) = \varphi(a) \oplus \varphi(b)$
2) $\varphi(a \cdot b) = \varphi(a) * \varphi(b)$

1.41 Сформулируйте теорему о гомоморфизме колец. Приведите пример.

Теорема (о гомоморфизме колец)**.** Пусть K_1, K_2 – два кольца, $\varphi : K_1 \to K_2$ – гомомрфизм. Тогда

$$\underbrace{K_1 / \operatorname{Ker} \varphi}_{\text{факторкольцо}} \cong \underbrace{\operatorname{Im} \varphi}_{\text{кольцо}}$$

Пример. $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, любому целому числу сопоставляем его остаток от деления на число n, $\operatorname{Ker} \varphi = n\mathbb{Z}$.

1.42 Сформулируйте критерий того, что кольцо вычетов по модулю n является полем.

Утверждение. $\mathbb{Z}_p$ является полем $\Leftrightarrow p$ –простое.

1.43 Сформулируйте теорему о том, когда факторкольцо кольца многочленов над полем само является полем.

Теорема. Пусть P – поле, а $f(x) \in P[x]$. Тогда факторкольцо $P[x]/\langle f(x)\rangle$ является полем $\Leftrightarrow$ многочлен $f(x)$ – неприводим над P.

1.44 Дайте определение алгебраического элемента над полем.

Определение. Элемент $\alpha \in P$ называется алгебраическим элементом над полем $F \subset P$, если существует $f(x) \neq 0$ (многочлен, т.е. $f(x) \in F[x]$) : $f(\alpha) = 0$. Если это не так, то α – трансцендентный элемент над F.

Пример. Пусть $F = \mathbb{Q}$. И $\sqrt{2} \in \mathbb{R}$ – алгебраическое число: $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. Элемент $\pi \in \mathbb{R}$ – трансцендентный.

1.45 Сформулируйте утверждение о том, что любое конечное поле может быть реализовано как факторкольцо кольца многочленов по некоторому идеалу.

Теорема. Любое конечное поле F_q, где $q = p^n$, а p – простое можно, реализовать в виде $\mathbb{Z}_p[x]/\langle h(x)\rangle$, где $h(x)$ – неприводимый многочлен степени n над $\mathbb{Z}_p$.

1.46 Дайте определение линейного (векторного) пространства.

Пусть F – поле, пусть V – произвольное множество, на котором задано 2 операции: сложение и умножение на число (т.е. элемент из F). Это означает, что $\forall x, y \in V$ существует элемент $x+y \in V$ и $\forall \lambda \in F \, \exists \lambda \cdot x \in V$. Множество V называется линейным пространством, если выполнены следующие 8 свойств:

$\forall x, y, z \in V$ и $\forall \lambda, \mu \in F$:

1) $(x + y) + z = x + (y + z)$ – ассоциативность сложения.
2) Найдется нейтральный элемент по сложению: $\exists 0 \in V : \forall x \in V : x + 0 = 0 + x = x$
3) Существует противоположный элемент по сложению: $\forall x \in V \, \exists(-x) \in V : x + (-x) = 0$
4) $x + y = y + x$ – коммутативность сложения
5) $\forall x \in V : 1 \cdot x = x$, нейтральный $1 \in F_1$
6) Ассоциативность умножения на число: $\mu(\lambda x) = (\mu\lambda)x$
7) Дистрибутивность относительно сложения чисел: $(\lambda + \mu)x = \lambda x + \mu x$
8) Дистрибутивность относительно сложения векторов: $\lambda(x + y) = \lambda x + \lambda y$

1.47 Дайте определение базиса линейного (векторного) пространства.

Определение. Базисом линейного пространства V называется упорядоченный набор векторов $b_1, \dots, b_n$ такой, что:

1) $b_1, \dots, b_n$ – л.н.з.
2) Любой вектор из V представляется линейной комбинацией векторов $b_1, \dots, b_n$, то есть $\forall x \in V$ $x = x_1 b_1 + \dots x_n b_n$. При этом $x_1, \dots, x_n$ называется координатами вектора в базисе $b_1, \dots, b_n$.

1.48 Что такое размерность пространства?

Определение. Максимальное количество л.н.з. векторов в данном линейном пространстве V называется размерностью этого линейного пространства.

1.49 Дайте определение матрицы перехода от старого базиса линейного пространства к новому.

Определение. Матрицей перехода от базиса $\mathcal{A}$ к базису $\mathcal{B}$ называется матрица:

$$T_{\mathcal{A}\to\mathcal{B}} = \begin{pmatrix} t_{11} & \cdots & t_{1n} \\ \vdots & & \vdots \\ t_{n1} & \cdots & t_{nn} \end{pmatrix}$$

$$(b_1, \dots, b_n)_{1\times n} = (a_1, \dots, a_n) \cdot T_{\mathcal{A}\to\mathcal{B}}$$

$b = a \cdot T_{\mathcal{A}\to\mathcal{B}}$ – матричная форма записи определения матрицы перехода, где $b = (b_1, \dots, b_n)$, $a = (a_1, \dots, a_n)$

1.50 Выпишите формулу для описания изменения координат вектора при изменении базиса.

Утверждение. Пусть $x \in L$, $\mathcal{A}$ и $\mathcal{B}$ – базисы в L.
$x^a = (x_1^a, \dots, x_n^a)^T$ – столбец координат вектора x в базисе $\mathcal{A}$.
$x^b = (x_1^b, \dots, x_n^b)^T$ – столбец координат вектора x в базисе $\mathcal{B}$.
Тогда $x^b = T_{\mathcal{A}\to\mathcal{B}}^{-1} x^a \Leftrightarrow X' = T^{-1}X$, где X' – координаты в новом базисе.

1.51 Дайте определение подпространства в линейном пространстве.

Определение. Подмножество W векторного пространства V называется подпространством, если оно само является пространством относительно операций в V.

1.52 Дайте определения линейной оболочки конечного набора векторов и ранга системы векторов.

Определение. Множество $L(a_1, \dots, a_k) = \{\lambda_1 a_1 + \dots \lambda_k a_k \mid \lambda_i \in F\}$ – множество всех линейных комбинаций векторов $a_1, \dots, a_k$ называется линейной оболочкой набора $a_1, \dots, a_k$.

Определение. Рангом системы векторов $a_1, \dots, a_k$ в линейном пространстве называется размерность их линейной оболочки.

$$\mathrm{Rg}(a_1, \dots, a_k) = \dim(L(a_1, \dots, a_k))$$

1.53 Дайте определения суммы и прямой суммы подпространств.

Определение. Множество $H_1 + H_2 = \{x_1 + x_2 \mid x_1 \in H_1, x_2 \in H_2\}$ называется суммой подпространств H_1 и H_2.

Определение. Сумма подпространств $H_1 + H_2$ называется прямой и обозначается $H_1 \oplus H_2$, где $H_1 \cap H_2 = \{0\}$, т.е. тривиально.

1.54 Сформулируйте утверждение о связи размерности суммы и пересечения подпространств.

Утверждение. Пусть H_1 и H_2 – подпространства в L. Тогда:

$$\dim(H_1 + H_2) = \dim(H_1) + \dim(H_2) - \dim(H_1 \cap H_2)$$

1.55 Дайте определение билинейной формы.

Пусть V – линейное пространство над $\mathbb{R}$.

Определение. Функцию $b : V \times V \to \mathbb{R}$ называют билинейной формой, если $\forall \alpha, \beta \in \mathbb{R}$:

1) $b(\alpha x + \beta y, z) = \alpha b(x, z) + \beta b(y, z)$
2) $b(x, \alpha y + \beta z) = \alpha b(x, y) + \beta b(x, z)$

1.56 Как меняется матрица билинейной формы при замене базиса? Как меняется матрица квадратичной формы при замене базиса?

Утверждение. Пусть U – матрица перехода от базиса e к базису f. Пусть B_e – матрица билинейной формы в базисе e. Тогда:

$$B_f = U^T B_e U$$