Алгебра. Определения и доказательства 3

Арунова Анастасия

Содержание

1 Определения

1.1 Какие бинарные операции называются ассоциативными, а какие коммутативными?

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

$*$ – 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 Сформулируйте два свойства гомоморфизма. Приведите пример.

Свойства гомоморфизма:

1) Нейтральный элемент переходит в нейтральный элемент ("единица"переходит в "единицу"), т.е. $f(e_G) = e_F$, где $f : G \to F$.

2) $f(a^{-1}) = (f(a))^{-1}$

Пример. $G_1 = (\mathbb{R}_+, \cdot)$, $G_2 = (\mathbb{R}, +)$ и гомоморфизмом $f = \ln x$.

1.11 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.

1.12 Дайте определение таблицы Кэли.

Определение. Таблица Кэли – это матрица из попарных произведений элементов группы (полугруппы и т.д.)

	g_1	g_2	$\dots$	g_n
g_1	$g_1 \cdot g_1$	$g_1 \cdot g_2$	$\dots$	$g_1 \cdot g_n$
g_2	$g_2 \cdot g_1$	$g_2 \cdot g_2$	$\dots$	$g_2 \cdot g_n$
$\vdots$	$\vdots$	$\vdots$	$\dots$	$\vdots$
g_n	$g_n \cdot g_1$	$g_n \cdot g_2$	$\dots$	$g_n \cdot g_n$

1.13 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.

1.14 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.

1.15 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).

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

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

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

1.16 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 $k \in \mathbb{N} \cup \{0\}$.

1.17 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: $Hg = \{h \cdot g \mid h \in H\}$).

1.18 Дайте определение нормальной подгруппы.

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

1.19 Что такое индекс подгруппы?

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

1.20 Сформулируйте теорему Лагранжа.

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

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

1.21 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

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

1.22 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) $\forall g \in G\ gHg^{-1} = H$

1.23 Сформулируйте определение простой группы.

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

1.24 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.

1.25 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

1.26 Сформулируйте критерий нормальности подгруппы, использующий понятие ядра гомоморфизма.

Утверждение. H – нормальная подгруппа в $G \Leftrightarrow H = \ker f$, f – гомоморфизм.

1.27 Сформулируйте теорему о гомоморфизме групп. Приведите пример.

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

Пример:

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

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

1.28 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

1.29 Сформулируйте определение автоморфизма и внутреннего автоморфизма.

Определение. Автоморфизм – это изоморфизм из G в G.

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

1.30 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 $\{1, -1\}$.

1.31 Что можно сказать про факторгруппу группы по её центру?

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

1.32 Сформулируйте теорему Кэли.

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

1.33 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: $\forall a, b, c$

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

1.34 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.

1.35 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.

1.36 Какие элементы кольца называются обратимыми?

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

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

1.38 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.

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

1.40 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 $P_0 \cong \mathbb{Q}$.

1.41 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.

1.42 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) $\varphi(a \cdot b) = \varphi(a) * \varphi(b)$

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

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, $\ker\varphi = n\mathbb{Z}$.

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

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

1.45 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.

1.46 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.

1.47 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 $\mathbb{Z}_p$.

1.48 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: $\lambda(x + y) = \lambda x + \lambda y$

1.49 Дайте определение базиса линейного (векторного) пространства.

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

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

1.50 Что такое размерность пространства?

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

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

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

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

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

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

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

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

1.53 Дайте определение подпространства в линейном пространстве.

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

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

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

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

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

1.55 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.

1.56 Сформулируйте утверждение о связи размерности суммы и пересечения подпространств.

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

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

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

1.58 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:

$$B_f = U^T B_e U$$

2 Доказательства

2.1 Сформулируйте и докажите утверждение о связи порядка элемента, порождающего циклическую группу, с порядком группы.

Утверждение. Пусть G – группа и $g \in G$. Тогда $|\langle g \rangle| = \mathrm{ord}(g)$

Доказательство. Заметим, что если $\forall k, s \in \mathbb{N}\ g^k = g^s \Rightarrow g^{k-s} = e$ (т.к. $\exists g^{-1}$), то $g \leq k - s \Rightarrow$ если g имеет бесконечный порядок, то все элементы g^n, $n \in \mathbb{Z}$ различны $\Rightarrow \langle g \rangle$ содержит бесконечного много элементов $\Rightarrow$ в бесконечном случае доказано.

Если же $\mathrm{ord}(g) = m$, то из минимальности $m \in N \Rightarrow e = g^0, g = g^n, \ldots, g^{m-1}$ попарно различны. Покажем, что $\langle g \rangle = \{e, g, g^2, \ldots, g^{m-1}\}$. Т.к. $\forall n \in \mathbb{Z}$ представимо в виде $n = qm + r$, где $0 \leq r < m$, $g^n = g^{qm+r} = (g^m)^q \cdot g^r = e^q \cdot g^r = g^r \Rightarrow \langle g \rangle = \{e, g, \ldots, g^{m-1}\}$ и $|\langle g \rangle| = m = \mathrm{ord}(g)$. □

2.2 Сформулируйте и докажите 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 $k \in \mathbb{N} \cup \{0\}$.

Доказательство. $k\mathbb{Z}$ является подгруппой. Докажем, что других нет.

Если $H = \{0\}$ (H – подгруппа, 0 – нейтральный элемент), то положим, что $k = 0$. Иначе $k = \min(H \cap \mathbb{N})$ ($\neq \varnothing$, т.к. $H \neq \{0\}$). Тогда $k\mathbb{Z} \subseteq H$.

Рассмотрим $a \in H$ и $a = qk + r$, $0 \leq r < k$. Тогда $r = \underbrace{a}_{\in H} - \underbrace{qk}_{\in H} \in H \Rightarrow r = 0$ (так как $r < k = \min(H \cap \mathbb{N})$). Получаем, что $a = qk \Rightarrow H \subseteq k\mathbb{Z}$.

Доказана принадлежность в обе стороны: $k\mathbb{Z} \subseteq H$ и $H \subseteq k\mathbb{Z}$. Значит, $k\mathbb{Z} = H$. □

2.3 Сформулируйте и докажите теорему Лагранжа (включая две леммы).

Лемма. Левые смежные классы G по подгруппе H либо не пересекаются, либо совпадают:

$$\forall g_1, g_2 \in G \text{ либо } g_1H = g_2H, \text{ либо } g_1H \cap g_2H = \varnothing$$

Доказательство. Докажем, что если классы пересекаются, то они совпадают. Если $g_1H \cap g_2H \neq \varnothing$, то $\exists h_1, h_2 \in H : g_1 \cdot h_1 = g_2 \cdot h_2 \Rightarrow g_1 = g_2 \cdot \underbrace{h_2 \cdot h_1^{-1}}_{\in H} \Rightarrow g_1H = g_2 \underbrace{h_2 h_1^{-1} H}_{\text{лежит в } H} \in g_2H \Rightarrow g_1H \subseteq g_2H$. Аналогично есть обратное включение $\Rightarrow g_1H = g_2H$. □

Лемма. $|gH| = |H|$, $\forall g \in G$ (и любой конечной подгруппы H).

Доказательство. Пусть $H = \{h_1, \ldots, h_n\}$, H – конечная подгруппа. Тогда смежный класс $gH = \{g \cdot h \mid h \in H\} =$
$= \{gh_1, \ldots, gh_n\}$. Тогда $|gH| \leq |H|$ (т.к. некоторые из $gh_1, \ldots, gh_n$ могут совпасть).

Предположим, что $|gH| < |H|$. Т.е. найдутся такие элементы $h_1, h_2 \in H$, что $h_1 \neq h_2$ и выполнено $gh_1 = gh_2$. Но тогда

$$gh_1 = gh_2 \Rightarrow g^{-1}gh_1 = g^{-1}gh_2 \Rightarrow h_1 = h_2$$

Получили противоречие. Следовательно, $|gH| = |H|$. □

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

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

Доказательство. Любой элемент группы G лежит в некотором левом смежном классе по H (gH). Т.к. левые смежные классы не пересекаются и любой из них содержит по $|H|$ элементов, группа G распределяется на непересекающиеся левые смежные классы порядка $|H| \Rightarrow |G| = |H| \cdot [G : H]$. □

2.4 Докажите, что гомоморфизм инъективен тогда и только тогда, когда его ядро тривиально.

Утверждение. Пусть $f : G \to F$ – гомоморфизм. Тогда f – инъективно (является мономорфизмом) $\Leftrightarrow \ker f = e_G$.

Доказательство.

Необходимость.

Дано: f – инъективно

Доказать: $\ker f = e_G$

$\forall x_1 \neq x_2 : f(x_1) \neq f(x_2) \Rightarrow f(e_G) = e_F$ (и для $x \in G$ и $x \neq e_G$ $f(x) \neq f(e_G) = e_F$)

Достаточность.

Дано: $\ker f = e_G$

Доказать: f – инъективно

Предположим, что $\exists x_1 \neq x_2 : f(x_1) = f(x_2)$. Тогда

$$f(x_1x_2^{-1}) = e_F = f(x_1) \cdot f(x_2^{-1}) = f(x_1) \cdot f(x_2)^{-1} \Rightarrow x_1 \cdot x_2^{-1} = e_G \Leftrightarrow x_1 = x_2$$

Противоречие с предположением $\Rightarrow f$ – мономорфизм (инъективно). □

2.5 Сформулируйте и докажите 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) $\forall g \in G\ gHg^{-1} = H$

Доказательство.

1) (1) $\Rightarrow$ (2)
   Т.к. $gH = Hg$, то $\forall h \in H\ gh = hg \Rightarrow ghg^{-1} = h \in H \Rightarrow gHg^{-1} \subseteq H$

2) (2) $\Rightarrow$ (3)
   Для $\forall h \in H\ h = gg^{-1}hgg^{-1} = g(g^{-1}hg)g^{-1} = g\underbrace{((g^{-1})h(g^{-1})^{-1})}_{\in H}g^{-1} \in gHg^{-1}$.
   Тогда $H \subseteq gHg^{-1}$, и, т.к. $gHg^{-1} \subseteq H$, $H = gHg^{-1}$

3) (3) $\Rightarrow$ (1)
   $gHg^{-1} = H \Leftrightarrow gHg^{-1}g = Hg \Leftrightarrow gH = Hg$ – условие нормальности.

□

2.6 Сформулируйте и докажите критерий нормальности подгруппы, использующий понятие ядра гомоморфизма.

Утверждение. H – нормальная подгруппа в $G \Leftrightarrow H = \ker f$, f – гомоморфизм.

Доказательство.

Необходимость.

Дано: H – нормальная подгруппа в G

Доказать: существует гомоморфизм f такой, что $H = \ker f$

В роли гомоморфизма f может выступать естественный гомоморфизм $\varepsilon : G \to G/H$. Он существует, т.к. H – нормальная подгруппа и G/H корректно определена. $\ker f$ – это множество всех элементов, которые перешли в $eH = H$ – исходная нормальная подгруппа.

Достаточность.

Дано: $H = \ker f$

Доказать: H – нормальная подгруппа в G

Пусть $f : G \to F$ – гомоморфизм. Покажем, что $\forall g \in G$ и $\forall z \in \ker f$ выполняется $g^{-1}zg \in \ker f$
$f(g^{-1}zg) = f(g^{-1})f(z)f(g) \overset{\text{св-во гомоморф.}}{=} f(g)^{-1}\underbrace{f(z)}_{e_F}f(g) = (f(g))^{-1}f(g) = e_F \overset{\text{опр.}}{\Rightarrow} g^{-1}zg \in \ker f$.

Так как $g^{-1}\ker fg \subseteq \ker f$, $\ker f$ – нормальная группа. □

2.7 Сформулируйте и докажите теорему о гомоморфизме групп.

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

Доказательство. Рассмотрим отображение $\tau : G/\ker f \to F$, заданное формулой

$$\tau(g \ker f) = f(g) \in \operatorname{Im} f$$

где $g \ker f$ – смежный класс $H = \ker f$.

Докажем, что τ и есть исходный изоморфизм. Проверим корректность (т.е. покажем, что τ не зависит от выбора представителя смежного класса):

$$\forall h_1, h_2 \in \ker f \; f(gh_1) = f(g)f(h_1) = f(g) \cdot e_F = f(g) = f(g) \cdot \underbrace{f(h_2)}_{e_F} = f(gh_2)$$

Значит, τ – определён корректно.

Отображение τ сюръективно ($\tau : G/\ker f \to \operatorname{Im} f$) и покажем, что оно инъективно.

По утверждению $f(g) = e_F \Leftrightarrow g \in \ker f = H$, т.е. ядро гомоморфизма состоит только из нейтрального элемента в факторгруппе. Воспользуемся критерием инъективности: τ – инъективно тогда и только тогда, когда $\ker \tau$ тривиально (состоит из $e \cdot \ker f$) $\Rightarrow \tau$ – биективно.

Остаётся проверить, что τ – гомоморфизм:

$$\tau((g_1 \ker f) \cdot (g_2 \cdot \ker f)) = \tau(g_1 g_2 \ker f) = f(g_1 g_2) = f(g_1)f(g_2) = \tau(g_1 \ker f)\tau(g_2 \ker f)$$

$\uparrow$ по определению произведения в факторгруппе; $\uparrow$ по определению τ; $\uparrow$ f – гомоморфизм; $\uparrow$ по определению τ

Таким образом, τ – биективный гомоморфизм, т.е. изоморфизм. □

2.8 Докажите, что центр группы является её нормальной подгруппой.

Утверждение. $Z(G)$ всегда является нормальной подгруппой в G.

Доказательство. Покажем, что $Z(G)$ является подгруппой. Для того, чтобы H было подгруппой нужно, чтобы $\forall a, b \in H \; ab^{-1} \in H$. Для того, чтобы проверить:

- что $e \in H$, берём $b = a \Rightarrow aa^{-1} = e \in H$
- что $ab \in H$, берём $b = b^{-1} \Rightarrow ab \in H$
- что $a^{-1} \in H$, берём $a = e, b = a \Rightarrow a \in H$

1) Проверим, что $\forall a, b \in Z(G)$ выполнено $ab^{-1} \in Z(G)$.

$$ab^{-1}g = ab^{-1}(g^{-1})^{-1} = a(g^{-1}b)^{-1} \overset{b \in Z(G)}{=} a(bg^{-1})^{-1} = a(g^{-1})^{-1}b^{-1} = agb^{-1} \overset{a \in Z(G)}{=} gab^{-1}$$

2) Это нормальная подгруппа, т.к. элементы коммутируют с любыми из G и $gZ(G) = Z(G)g$.

□

2.9 Сформулируйте и докажите утверждение о том, чему изоморфна факторгруппа группы по её центру.

Утверждение. $G/Z(G) \cong I_{nn}(G)$

Доказательство. Факторгруппа $G/Z(G)$ является нормальной подгруппой. Рассмотрим отображение $f : G \to \mathrm{Aut}(G)$, заданнное формулой $f : g \mapsto \varphi_g(h) = ghg^{-1}$.

Тогда $\mathrm{Im}\, f = I_{nn}(G)$ по определению и $\ker f = Z(G)$, т.к. $ghg^{-1} = h \Leftrightarrow gh = hg$ ($\varphi_g(h) = id(h)$ – нейтральный элемент во второй группе).

Тогда $gh = hg$ верно для тех элементов, которые коммутируют с любым, т.е. элементов центра.

Применим теорему о гомоморфизме групп:

$$G/\ker f \cong \mathrm{Im}\, f \Leftrightarrow G/Z(G) \cong I_{nn}(G) \qquad \square$$

2.10 Сформулируйте и докажите теорему Кэли.

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

Доказательство. Пусть $|G| = n$, и $\forall a \in G$ рассмотрим отображение $L_a : G \to G$, определённое формулой $L_a(g) = a \cdot g$ (умножение слева на a). Покажем, что L_a – это биекция.

Пусть $e, g_1, g_2, \ldots, g_{n-1}$ элементы группы тогда $a \cdot e, a \cdot g, \ldots, a \cdot g_{n-1}$ – те же самые элементы, но в другом порядке ($ag_i = ag_j \Leftrightarrow a^{-1}ag_i = a^{-1}ag_j \Leftrightarrow g_i = g_j$) $\Rightarrow L_a$ – перестановка элементов группы.

Существует нейтральный элемент: $id = L_e$.

По ассоциативности в G: $L_{ab}(g) = (ab)g = a(bg) \Leftrightarrow L_{ab} = L_a \circ L_b$.

При этом относительно операции композиции отображений: $\forall L_a\ \exists (L_a)^{-1} = L_{a^{-1}}$

Таким образом, множество $L_e, L_{g_1}, L_{g_2}, \ldots, L_{g_{n-1}}$ образуют группу H в группе $S(G)$ всех биективных отображений G на себя, т.е. в S_n.

Искомый изоморфизм: $\underbrace{a}_{\in G} \mapsto \underbrace{L_a}_{\in H \subseteq S_n}$ $\square$

2.11 Докажите, что характеристика поля может быть либо простым числом, либо нулем.

Утверждение. $\mathrm{char}\, P = \begin{cases} 0 \\ p,\ p - \text{простое} \end{cases}$

Доказательство. Пусть $p \neq 0 \Rightarrow p \geq 2$ ($p \neq 1$, т.к. $1 \neq 0$)

Если $p = mk$, где $1 < m, k < p$, то $0 = \overbrace{\overline{1} + \ldots + \overline{1}}^{mk} = \overbrace{(\overline{1} + \ldots + \overline{1})}^{m}\overbrace{(\overline{1} + \ldots + \overline{1})}^{k}$. Обе скобки $\neq 0$, так как p по определению минимальное натуральное число при котором $\overline{1} + \ldots + \overline{1} = 0$, а $m, k < p$ $\Rightarrow$ m и k делители нуля, а их нет в поле по определению. $\square$

2.12 Сформулируйте и докажите 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 $P_0 \cong \mathbb{Q}$.

Доказательство. Рассмотрим $1 \in P$ (нейтральный элемент по умножению) $\Rightarrow \langle 1 \rangle \subseteq (P, +)$, $\langle 1 \rangle$ – циклическая группа по сложению, порождённая 1.

Кольцо $\langle 1 \rangle$ является подкольцом в P.

Т.к. любое подполе поля P содержит 1, то оно содержит и $\langle 1 \rangle$, т.е. $\langle 1 \rangle \subseteq P_0$.

1) Если $\operatorname{char} P = p > 0$, то $\langle 1 \rangle \cong \mathbb{Z}_p$ – поле $\Rightarrow P_0 = \langle 1 \rangle \cong \mathbb{Z}_p$

   Пример. $\underbrace{\mathbb{Z}_p}_{P_0} \subset \underbrace{\mathbb{Z}_p(x)}_{P}$

2) Если $\operatorname{char} P = 0$, то $\langle 1 \rangle \cong \mathbb{Z}$ (это не поле), значит, в P_0 должны быть все дроби $\dfrac{a}{b}$, где $a, b \in \langle 1 \rangle, b \neq 0$. Они все образуют подполе изоморфное $\mathbb{Q}$.

$\square$

2.13 Сформулируйте и докажите критерий того, что кольцо вычетов по модулю n является полем.

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

Доказательство. Для любого n $\mathbb{Z}_n$ является кольцом с 1. Если n является составным, то $n = mk$, $1 \leq m, k \leq n$, и, следовательно, $\overline{m}\overline{k} = \overline{n} = \overline{0} \Rightarrow$ в кольце есть делители нуля $\Rightarrow$ это не поле.

Если p – простое, рассмотрим $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ – все классы вычетов, кроме $\overline{0}$. Возьмём произвольный элемент $\overline{s}$ и докажем, что $\exists\, \overline{s}^{-1} : \overline{s} \cdot \overline{s}^{-1} = \overline{1}$. Рассмотрим множество $A = \{\overline{s} \cdot \overline{1}, \overline{s} \cdot \overline{2}, \ldots, \overline{s} \cdot \overline{p-1}\}$ в A нет $\overline{0}$ (т.к. p – простое, а среди чисел нет 0 или кратных 0). Заметим, что в A стоят те же элементы, но в другом порядке (если $\overline{k_1} \cdot \overline{s} = \overline{k_2} \cdot \overline{s} \Leftrightarrow (\overline{k_1} - \overline{k_2})\overline{s} = \overline{0}$, а это возможно только при $\overline{k_1} = \overline{k_2}$) $\Rightarrow$ в наборе $\overline{s}, \overline{s} \cdot \overline{2}, \ldots, \overline{s} \cdot \overline{p-1}$ найдётся 1 $\Rightarrow$ существует элемент $\overline{s}^{-1} : \overline{s} \cdot \overline{s}^{-1} = \overline{1} \Rightarrow \overline{s}$ (он произвольный) обратим. $\square$

2.14 Докажите, что ядро гомоморфизма колец является идеалом.

Лемма. $\ker\varphi$, где φ – гомоморфизм колец, всегда является идеалом в кольце K_1 ($\varphi : K_1 \to K_2$)

Доказательство.

Идеал:

1) Подгруппа в $(K_1, +)$
2) $\forall a \in \ker\varphi\ \forall r \in K_1\ ar \in \ker\varphi$ и $ra \in \ker\varphi$

Любой гомоморфизм колец является гомоморфизмом их аддитивных групп $(K_1, +)$ и $(K_2, +) \Rightarrow \ker\varphi$ является нормальной подгруппой в $(K_1, +)$ ($(K_1, +)$ коммутативна). Пусть $a \in \ker\varphi$, т.е. $\varphi(a) = 0$. Возьмём ar и рассмотрим выражение $\varphi(ar) = \varphi(a) \cdot \varphi(r) = 0 \cdot \varphi(r) = 0$. И аналогично $\varphi(ra) = \varphi(r) \cdot 0 = 0$. □

2.15 Сформулируйте и докажите утверждение 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.

Доказательство. Если $f(x) = f_1(x) \cdot f_2(x)$ (т.е. не является неприводимым), где $0 < \deg f_i < \deg f$, $\overline{f}_1, \overline{f}_2 \in P[x]/\langle f(x)\rangle$, отличаются от нуля, но $\overline{f_1(x)} \cdot \overline{f_2(x)} = \overline{f(x)} = \overline{0} \Rightarrow$ в $P[x]/\langle f(x)\rangle$ есть делители нуля и это не поле.

Покажем, что если $f(x)$ неприводим, то любой класс вычетов $\overline{a(x)} \neq \overline{0}$ обратим. Представитель $\overline{a(x)}$ это некоторый многочлен $a(x)$ с $\deg a(x) < \deg f(x)$. Т.к. $f(x)$ неприводим, он взаимно прост с $a(x) \Rightarrow \exists b(x), c(x) : a \cdot b + c \cdot f = 1$ (НОД), т.е. $\overline{a}\overline{b} + \overline{c}\overline{f} = \overline{1}$, т.е. $\overline{a} \cdot \overline{b} = \overline{1}\langle f(x)\rangle$, т.е. $\overline{b}$ – обратный элемент к $\overline{a}$ в $P[x]/\langle f(x)\rangle$. □

2.16 Выпишите и докажите формулу для описания изменения координат вектора при изменении базиса.

Утверждение. Пусть $x \in L$, $\mathcal{A}$ и $\mathcal{B}$ – базисы в L.

$x^a = (x_1^a, \ldots, x_n^a)^T$ – столбец координат вектора x в базисе $\mathcal{A}$.

$x^b = (x_1^b, \ldots, x_n^b)^T$ – столбец координат вектора x в базисе $\mathcal{B}$.

Тогда $x^b = T^{-1}_{\mathcal{A}\to\mathcal{B}}\, x^a \Leftrightarrow X' = T^{-1}X$, где X' – координаты в новом базисе.

Доказательство. Докажем, что $x^b = T^{-1}_{\mathcal{A}\to\mathcal{B}}\, x^a$ (из невырожденности матрицы перехода будет следовать нужная формула).

$$x = a \cdot x^a = (a_1, \ldots, a_n) \begin{pmatrix} x_1^a \\ \vdots \\ x_n^a \end{pmatrix} = x_1^a a_1 + \ldots + x_n^a a_n = bx^b$$

$$b = a \cdot T_{\mathcal{A}\to\mathcal{B}} \Rightarrow a \cdot x^a = b \cdot x^b, ax^a = a \cdot T_{\mathcal{A}\to\mathcal{B}} \cdot x^b$$

$$x^a = T_{\mathcal{A}\to\mathcal{B}} \cdot x^b \Rightarrow x^b = T^{-1}_{\mathcal{A}\to\mathcal{B}} \cdot x^a \qquad \square$$

2.17 Выпишите формулу для преобразования матрицы билинейной формы при замене базиса и докажите её.

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

$$B_f = U^T B_e U$$

Доказательство. $b(x, y) = (x^e)^T \cdot B_e \cdot y^e$, где x^e – столбец координат в базисе e

$x^e = Ux^f$ (x^e – старые координаты, а x^f – новые)

$y^e = Uy^f$ (y^e – старые координаты, а y^f – новые)

$$(Ux^f)^T \cdot B_e \cdot (U \cdot y^f) = (x^f)^T \cdot \underbrace{U^T \cdot B_e \cdot U}_{B_f} \cdot y^f = (x^f)^T B_f y^f \Rightarrow B_f = U^T B_e U \qquad \square$$