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 $|\langle g \rangle| = \text{ord}(g)$

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 $\text{ord}\, g \leq k - s \Rightarrow$ 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 $\text{ord}(g) = m$, 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 $|\langle g \rangle| = m = \text{ord}(g)$. □

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:

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

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

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

Доказательство. Пусть $H = \{h_1, \dots, h_n\}$, H – конечная подгруппа. Тогда смежный класс

$$gH = \{g \cdot h \mid h \in H\} = \{gh_1, \dots, gh_n\}$$

Тогда $|gH| \leq |H|$ (т.к. некоторые из $gh_1, \dots, gh_n$ 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) $\Leftrightarrow \operatorname{Ker} f = e_G$.

Доказательство.

Необходимость. Дано: f – инъективно

Доказать: $\operatorname{Ker} f = e_G$

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

Достаточность. Дано: $\operatorname{Ker} f = e_G$

Доказать: f – инъективно

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

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

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 $G \Leftrightarrow H = \operatorname{Ker} f$, f – гомоморфизм.

Доказательство.

Необходимость. Дано: H – нормальная подгруппа в G

Доказать: существует гомоморфизм f такой, что $H = \operatorname{Ker} f$

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. $\operatorname{Ker} f$ – это множество всех элементов, которые перешли в $eH = H$ – исходная нормальная подгруппа.

Достаточность. Дано: H – нормальная подгруппа в $GH = \operatorname{Ker} f$

Доказать: H – нормальная подгруппа в G

Пусть $f : G \to F$ – гомоморфизм. Покажем, что $\forall g \in G$ и $\forall z \in \operatorname{Ker} f$ выполняется $g^{-1}zg \in \operatorname{Ker} f$

$f(g^{-1}zg) = f(g^{-1})f(z)f(g) \overset{\text{св-во гомоморф.}}{=} f(g)^{-1}\underbrace{f(z)}_{e_F}f(g) = (f(g))^{-1}f(g) = e_F \overset{\text{опр.}}{\Rightarrow} g^{-1}zg \in \operatorname{Ker} f$.

Так как $g^{-1} \operatorname{Ker} fg \subseteq \operatorname{Ker} f$, $\operatorname{Ker} f$ – 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 $G/\operatorname{Ker} f$, 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.

Доказательство. Рассмотрим отображение $\tau : G/\operatorname{Ker} f \to F$, заданное формулой

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

где $g \operatorname{Ker} f$ – смежный класс $H = \operatorname{Ker} f$.

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

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

Значит, τ – определён корректно.

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

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

Остаётся проверить, что τ – гомоморфизм:

$$\tau((g_1 \operatorname{Ker} f) \cdot (g_2 \cdot \operatorname{Ker} f)) \underset{\substack{\text{по определению}\\ \text{произведения в}\\ \text{факторгруппе}}}{=} \tau(g_1 g_2 \operatorname{Ker} f) \underset{\text{по определению } \tau}{=} f(g_1 g_2) \underset{f \text{ – гомоморфизм}}{=} f(g_1) f(g_2) \underset{\text{по определению } \tau}{=} \tau(g_1 \operatorname{Ker} f)\tau(g_2 \operatorname{Ker} f)$$

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 $\mathrm{Ker}\, f = Z(G)$, 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:

$$G/\,\mathrm{Ker}\, f \cong \mathrm{Im}\, f \Leftrightarrow G/Z(G) \cong I_{nn}(G)$$ □

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: $\underbrace{a}_{\in G} \mapsto \underbrace{L_a}_{\in H \subseteq S_n}$ □

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

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 $\mathbb{Q}$.

□

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. □

2.14 Докажите, что ядро гомоморфизма колец является идеалом.

Лемма. $\operatorname{Ker}\varphi$, 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) $\forall a \in \operatorname{Ker}\varphi\, \forall r \in K_1\; ar \in \operatorname{Ker}\varphi$ и $ra \in \operatorname{Ker}\varphi$

Любой гомоморфизм колец является гомоморфизмом их аддитивных групп $(K_1, +)$ и $(K_2, +) \Rightarrow \operatorname{Ker}\varphi$ является нормальной подгруппой в $(K_1, +)$ ($(K_1, +)$ коммутативна). Пусть $a \in \operatorname{Ker}\varphi$, 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. $\overline{a} \cdot \overline{b} = \overline{1} \bmod \langle f(x)\rangle$, 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).

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

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

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

□

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)

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

□

2.18 Сформулируйте и докажите теорему о гомоморфизме колец.

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

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

Доказательство. Ядро $\operatorname{Ker}\varphi$ является идеалом (по лемме*) $\Rightarrow$ $K_1/\operatorname{Ker}\varphi$ корректно определён. Рассмотрим отображение $\tau : k_1/\operatorname{Ker}\varphi \to \operatorname{Im}\varphi$. Выполняется $\tau(a + I) = \varphi(a)$ из доказательства теоремы о гомоморфизме групп $\Rightarrow$ τ – корректно определено и является гомоморфизмом групп по сложению. Остаётся проверить, что τ сохраняет умножение:

$$\tau((a + I)(b + I)) = \tau(ab + I) = \varphi(ab) = \varphi(a) \cdot \varphi(b) = \tau(a + I) * \tau(b + I)$$

Значит, τ – гомоморфизм колец. И, т.к. τ является биекцией (из теоремы о гомомрфизме групп), то это изоморфизм (между $K_1/\operatorname{Ker}\varphi$ и $\operatorname{Im}\varphi$).

Лемма. * Ядро $\operatorname{Ker}\varphi$, где φ – гомоморфизм колец, всегда является идеалом в кольце K_1 ($\varphi : K_1 \to K_2$)

$\square$

2.19 Что такое сумма и прямая сумма подпространств? Сформулируйте и докажите критерий того, что сумма подпространств является прямой.

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.

Утверждение. $H_1 + H_2$ является прямой суммой $\Leftrightarrow \forall x \in H_1 + H_2$ единственным образом представляется $x_1 \in H_1$ и $x_2 \in H_2$ в виде $x = x_1 + x_2$.

Доказательство.

Необходимость. Дано: сумма прямая, т.е. $H_1 \cap H_2 = \{0\}$

Доказать: $x = x_1 + x_2$ представляется единственным образом

Предположим, что есть 2 разложения: $x = x_1 + x_2$ и $x = y_1 + y_2$, $x_1, y_1 \in H_1$, $x_2, y_2 \in H_2$. Вычтем их друг из друга:

$$x_1 - y_1 = y_2 - x_2 = 0 \Rightarrow \begin{cases} x_1 = y_1 \\ x_2 = y_2 \end{cases}$$

Достаточность. Дано: $x = x_1 + x_2$ представляется единственным образом

Доказать: сумма прямая

Если мы предположим, что $\exists x \neq 0 : x \in H_1 \cap H_2$, то $\forall \alpha \in F : \alpha x \in H_1$ и $\alpha x \in H_2$. Тогда $\forall \beta \in F : x = x - \beta x + \beta x = \underbrace{(1-\beta)x}_{\in H_1} + \underbrace{\beta x}_{\in H_2} \Rightarrow$ представление не единственно. $\square$

2.20 Сформулируйте и докажите утверждение о связи размерности суммы и пересечения подпространств.

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

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