

Доказательства к кр по линалу 3 модуля.

1. Сформулируйте и докажите утверждение о том, какими могут быть подгруппы группы целых чисел по сложению.

\forall подгруппа в $(\mathbb{Z}, +)$ имеет вид $k\mathbb{Z}$ для некоторых $k \in \mathbb{N} \cup \{0\}$

□

Если $H = \{0\}$, то положим $k = 0$. Иначе: $k = \min(H \cap \mathbb{N}) \rightarrow$ и очевидно, что $k\mathbb{Z} \subseteq H$. Если возьмем $a \in H$ и разделим a на k с остатком: $a = qk + r$, где $0 \leq r < k \Rightarrow r = a - q \cdot k \in H \Rightarrow r = 0 \Rightarrow a = q \cdot k$, то есть всегда $H = k\mathbb{Z}$

■

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

Лемма 1: $\forall g_1, g_2 \in G$ либо $g_1H = g_2H$, либо $g_1H \cap g_2H = \emptyset$

□

Если $g_1H \cap g_2H \neq \emptyset$, то $g_1H = g_2h_2h_1^{-1}H \subseteq g_2H$ и аналогично в обратную сторону $\exists h_1, h_2 : g_1h_1 = g_2h_2$, так как пересечение не пусто $\Rightarrow g_1 = g_2h_2h_1^{-1}$

■

Лемма 2: $|gH| = |H| \forall g \in G, \forall$ конечной подгруппы H

□

$|gH| \leq |H|$, так как $gH = \{gh | h \in H\}$

Если $gh_1 = gh_2 \Rightarrow g^{-1}gh_1 = g^{-1}gh_2 \Rightarrow h_1 = h_2 \Rightarrow$ нет совпадений и $|gH| = |H|$

■

Теорема Лагранжа:

Пусть G – конечная группа и $H \subseteq G$ – подгруппа. Тогда $|G| = |H| \cdot [G : H]$

□

\forall элемент группы G лежит в своем левом смежном классе по H и смежные классы не пересекаются (по лемме 1) и \forall из них содержит $|H|$ элементов (по лемме 2)

■

Следствие 1: Пусть G – конечная группа и $g \in G$. Тогда $\text{ord}(g)$ делит $|G|$

Следствие 2: Пусть G – конечная группа. Тогда $g^{|G|} = e$

Следствие 3 (малая теорема Ферма): Пусть \bar{a} – ненулевой вычет по простому модулю p .

Тогда $\bar{a}^{p-1} \equiv 1 \pmod{p}$

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

Гомоморфизм α инъективен тогда и только тогда, когда $\text{Ker } \alpha = \{e_1\}$

Доказательство.

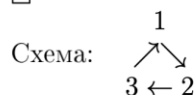
Поскольку $\alpha(e_1) = e_2$, указанное условие необходимо. С другой стороны, если $\alpha(g) = \alpha(g')$, то $\alpha(gg'^{-1}) = e_2 \Rightarrow gg'^{-1} \in \text{Ker } \alpha$ и если ядро тривиально, $g = g'$ и отображение инъективно.

4. Сформулируйте и докажите критерий нормальности подгруппы, использующий сопряжение.

Пусть $H \subseteq G$ – подгруппа в группе G . Тогда 3 условия эквивалентны:

1. H нормальна
2. $\forall g \in G \ gHg^{-1} \subseteq H$ ($gHg^{-1} = \{ghg^{-1} | h \in H\}$)
3. $\forall g \in G \ gHg^{-1} = H$

□



$1 \rightarrow 2$ Пусть $h \in H$ и $g \in G$. Из определения $\Rightarrow \exists h, h' \in H : gh = h'g$
 $ghg^{-1} = h' \in H$, то есть $gHg^{-1} \subseteq H$

$2 \rightarrow 3$ Остается показать, что $H \subseteq gHg^{-1}$. Для $h \in H$ имеем $h = gg^{-1}hgg^{-1} = g(g^{-1}hg)g^{-1} \in gHg^{-1}$, так как $g^{-1}hg \in H$ (вместо g взяли g^{-1})

$3 \rightarrow 1$ $\forall g \in G$ по пункту 3 $gH = gHg^{-1}g \subseteq Hg$. Аналогично $Hg \subseteq gH \Rightarrow Hg = gH$ – по определению это нормальность.

■

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

H – нормальная подгруппа $\Leftrightarrow H = \text{Ker } f$, где f – некоторый гомоморфизм

□

Необходимость

Дано: H – нормальная подгруппа

Нужно доказать: $\exists f$ – гомоморфизм: $H = \text{Ker } f$

Это естественный гомоморфизм, сопоставляющий \forall элементу $a \in G$ его смежный класс aH

$\varepsilon : G \rightarrow G/H$

Тогда $\text{Ker } \varepsilon = eH = H$

Достаточность

$H = \text{Ker } f$

Ранее показали, что $\text{Ker } f$ – подгруппа.

Покажем, что $\text{Ker } f$ – нормальная подгруппа. Пусть $f : G \rightarrow F$ – гомоморфизм и $z \in \text{Ker } f$.

Тогда $f(g^{-1}zg) = f(g^{-1})f(z)f(g) = f(g^{-1})ef(g) = f(g^{-1}g) = f(e_G) = e_F$. То есть $\forall g \in G : g^{-1}Hg \subseteq H$, где $H = \text{Ker } f \Rightarrow$ по критерию $H = \text{Ker } f$ – нормальна

■

6. Сформулируйте и докажите теорему о гомоморфизме групп.

Пусть $f : G \rightarrow F$ – гомоморфизм групп. Тогда группа $Imf = \{a \in F | \exists g \in G, f(g) = a\}$ изоморфна фактор-группе $G/Kerf$

$Kerf = \{g \in G | f(g) = e_F\}$ ($Kerf$ – ядро гомоморфизма)

$$G/Kerf \simeq Imf$$

□

Рассмотрим $\tau : G/Kerf \rightarrow F$, заданное формулой $\tau(gKer(f)) = f(g) \in F$

$(gKer(f) = gH, \text{ где } H = Kerf)$

Проверим корректность:

$\forall h_1, h_2 \in Kerf$

$f(gh_1) = f(g)f(h_1) = f(g)e_F = f(g) = f(g)f(h_2) = f(gh_2)$, то есть значения τ не зависят от выбора представителя смежного класса.

Отображение τ сюръективно по построению и инъективно в силу того, что

$f(g) = e_F \Leftrightarrow g \in Kerf$ (то есть $gKerf = Kerf$)

Остается проверить, что τ – гомоморфизм

$$\tau((gKerf) \cdot (g'Kerf)) = \tau(gg'Kerf) = f(gg') = f(g) \cdot f(g') = \tau(gKerf) \cdot \tau(g'Kerf)$$

■

7. Докажите, что центр группы является её нормальной подгруппой.

$Z(G)$ является нормальной подгруппой G

□

1. Покажем, что $Z(G)$ – подгруппа, то есть $\forall a, b \in Z(G) a \cdot b^{-1} \in Z(G)$

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

2. Если $a \in Z(G)$ и $g, b \in G$

$$g^{-1}agb = g^{-1}gab = ab = ba = bag^{-1}g = bg^{-1}ag, \text{ то есть если элемент } a \in Z(G), \text{ то } g^{-1}ag \text{ тоже } \in Z(G).$$

А это по критерию означает нормальность.

■

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

$$G/Z(G) \simeq Inn(G)$$

□

Рассмотрим отображение $f : G \rightarrow Aut(G)$, которое задается формулой $\phi_g(h) = ghg^{-1}$. Тогда

$Imf = Inn(G)$ по определению. $Kerf = Z(G)$, так как $ghg^{-1} = ehe^{-1} = h \Leftrightarrow gh = hg$

\Rightarrow по теореме о гомоморфизме $G/Kerf \simeq Imf$, то есть $G/Z(G) \simeq Inn(G)$

■

9. Сформулируйте и докажите теорему Кэли.

\forall конечная группа порядка n изоморфна некоторой подгруппе группы S_n

□

Пусть $|G| = n$. $\forall a \in G$ рассмотрим отображение $L_a : G \rightarrow G$ по формуле: $L_a(g) = a \cdot g$

Пусть $e, g_1, g_2, \dots, g_{n-1}$ — элементы группы. Тогда $a, ag_1, ag_2, \dots, ag_{n-1}$ — те же элементы, но в другом порядке (если $ag_i = ag_j \Rightarrow g_i = g_j$, так как $\exists a^{-1} \forall a \in G$)

$\Rightarrow L_a$ — биективное отображение G в себя (то есть перестановка элементов g)

Эти отображения можно умножать (взяв композицию)

Есть единичный элемент: L_e

Обратным элементом к L_a является $L_{a^{-1}}$

Из ассоциативности в $G \Rightarrow L_{ab}(g) = (a \cdot b)g = a(b \cdot g) = L_a(L_b(g)) \Rightarrow$ множество $L_e, L_{g_1}, L_{g_2}, \dots, L_{g_{n-1}}$ образует подгруппу H в множестве всех биективных отображений G в себя, то есть $S(G)$

А изоморфизм устроен так: $a \mapsto L_a \in H$ это биекция и гомоморфизм

■

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

Определение Пусть P — поле. Характеристикой поля называется наименьшее $q \in \mathbb{N} : \underbrace{1 + 1 + \dots + 1}_q = 0$. Если такого q нет, то характеристика равно нулю

Обозначение: $\text{char}(P)$

Примеры

$$1. \text{char}(\mathbb{R}) = \text{char}(\mathbb{C}) = \text{char}(\mathbb{Q}) = 0$$

$$2. \text{char}(\mathbb{Z}_p) = p$$

Утверждение: $\text{char}(p) = \begin{cases} 0, \\ p, p - \text{простое} \end{cases}$

□ Пусть $p \neq 0 \Rightarrow p \geq 2(1 \neq 0)$

Если $p = m \cdot k$, где $1 \leq m, k < p$

$0 = \underbrace{1 + \dots + 1}_{m \cdot k} = \underbrace{(1 + \dots + 1)}_m \cdot \underbrace{(1 + \dots + 1)}_k$ так как $p = M \cdot k$ минимально, то обе скобки $\neq 0 \Rightarrow m$ и k — делители нуля — а их нет в поле по определению ■

11. Сформулируйте и докажите утверждение о том, каким будет простое подполе в зависимости от характеристики.

Пусть F — поле. F_0 — его простое подполе. Тогда:

1. Если $\text{char} F = p > 0$, то $F_0 \simeq \mathbb{Z}_p$

2. Если $\text{char} F = 0$, то $F_0 \simeq \mathbb{Q}$

□

$\langle 1 \rangle \subseteq (F, +)$, где $\langle 1 \rangle$ — циклическая подгруппа по сложению, порожденная 1 (то есть нейтральным элементом по умножению)

$|\langle 1 \rangle| = \text{char} F$

$\langle 1 \rangle$ — подкольцо в F . Так как \forall подполе F содержит 1 \Rightarrow оно содержит и $\langle 1 \rangle \subseteq F_0$

1. Если $\text{char} F = p > 0$, то $\langle 1 \rangle \simeq \mathbb{Z}_p$ — поле $\Rightarrow F_0 = \langle 1 \rangle \simeq \mathbb{Z}_p$

2. Если $\text{char} F = 0$, то $\langle 1 \rangle \simeq \mathbb{Z}$ — не поле. Но F_0 содержит и все дроби вида $\frac{a}{b}$, где $a, b \in \langle 1 \rangle, b \neq 0$ и они образуют поле, изоморфное \mathbb{Q} (\mathbb{Q} — поле частных для кольца \mathbb{Z})

■

12. Сформулируйте и докажите критерий того, что кольцо вычетов по модулю p является полем.

Меняем p на n !

\mathbb{Z}_k – поле $\Leftrightarrow k$ – простое

□

\mathbb{Z}_k – коммутативное кольцо с 1.

Если $k = p$ – простое, то в \mathbb{Z}_p^* (то есть $\mathbb{Z}_p \setminus \{0\}$ с операцией умножения) все элементы обратимы.

Рассмотрим $\overline{1}, \dots, \overline{p-1}$

Возьмем остаток \overline{s} и докажем, что $\exists \overline{s}^{-1}$

Рассмотрим $\{\overline{s}, \overline{s} \cdot \overline{2}, \overline{s} \cdot \overline{3}, \dots, \overline{s} \cdot \overline{p-1}\} = A$. Если $\overline{s} \neq 0 \Rightarrow \overline{k} \cdot \overline{s} \neq 0 \pmod p \Rightarrow$ в A нет нуля. Более того, это те же элементы, но в другом порядке. Если $\overline{k} \cdot \overline{s} = \overline{q} \cdot \overline{s} \Rightarrow (\overline{k} - \overline{q}) \cdot \overline{s} = \overline{0} \Rightarrow \overline{k} - \overline{q} = \overline{0} \Rightarrow$ в наборе $\overline{s}, \overline{s} \cdot \overline{2}, \overline{s} \cdot \overline{3}, \dots, \overline{s} \cdot \overline{p-1}$ найдется $1 \Rightarrow \overline{s} \cdot \overline{s}' = 1$, то есть \overline{s} обратим

■

13. Докажите, что ядро гомоморфизма колец является идеалом.

Лемма $\text{Ker}(\varphi)$, где φ – гомоморфизм колец, всегда является идеалом в кольце K_1 ($\varphi : K_1 \rightarrow K_2$)

□ Идеал:

1. Подгруппа в $(K_1, +)$

2. $\forall a \in \text{Ker}(\varphi) \forall r \in K_1 : a \cdot r \in \text{Ker}(\varphi) \wedge r \cdot a \in \text{Ker}(\varphi)$

Любой гомоморфизм колец является гомоморфизмом их аддитивных групп $\Rightarrow \text{Ker}(\varphi)$ является нормальной подгруппой в $(\text{Ker}_1, +)$.

Пусть $a \in \text{Ker}(\varphi)$ т. е. $\varphi(a) = 0$. Берем $a \cdot r$ и рассмотрим

$$\varphi(a \cdot r) = \varphi(a) \cdot \varphi(r) = 0 \cdot \varphi(r) = 0$$

И аналогично $\varphi(r \cdot a) = \varphi(r) \cdot 0 = 0$ ■

Лемма $r \cdot 0 = 0 \cdot r = 0$

$$\square r + 0 = r \Rightarrow r(r + 0) = r \cdot r \Rightarrow r^2 + r \cdot 0 = r^2 \mid + (-r^2)$$

$r \cdot 0 = 0$ ч. т. д. ■

14. Сформулируйте и докажите утверждение о том, когда факторкольцо кольца многочленов над полем само является полем.

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

Необходимость:

$F[x] / \langle f(x) \rangle$ – поле, доказать, что $f(x)$ – неприводим.

В поле нет делителей 0.

Так как $f(x)$ можно разложить на скобки, например, $q(x) * r(x)$

То получаем, что $q(x) * r(x) = 0$.

В поле нет делителей 0 \Rightarrow противоречие.

Многочлен неприводим.

Достаточность:

$f(x)$ – неприводим, доказать, что $F[x] / \langle f(x) \rangle$ – поле

$\forall g(x) \neq 0$ в этом факторкольце верно:

$\text{GCD}(f(x), g(x)) = 1$, по причине неприводимости $f(x)$

По обратному алгоритму Евклида: $\text{GCD}(f(x), g(x)) = v(x) * f(x) + u(x) * g(x)$

$v(x) * f(x) + u(x) * g(x) = 1$, причём в данном факторкольце мы знаем, что $f(x) * v(x) = 0$

$u(x) * g(x) = 1$

$g(x) = u^{-1}(x)$

Получается, $\forall g(x) \neq 0$ в этом факторкольце \exists обратный элемент $\Rightarrow F[x] / \langle f(x) \rangle$ является полем.

Ч. И. Т. Д. \square

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

Пусть $x \in V$, A и B – базисы в V . $x^a = \begin{pmatrix} x_1^a \\ \vdots \\ x_n^a \end{pmatrix}$ – столбец координат вектора x в базисе A ,

$x^b = \begin{pmatrix} x_1^b \\ \vdots \\ x_n^b \end{pmatrix}$ – столбец координат вектора x в базисе B . Тогда $x^b = T_{A \rightarrow B}^{-1} \cdot x^a$

□

Докажем, что $x^a = T_{A \rightarrow B} \cdot x^b$

$$x = \mathbb{A} \cdot x^a = (a_1, \dots, a_n) \cdot \begin{pmatrix} x_1^a \\ \vdots \\ x_n^a \end{pmatrix} = \mathbb{B} \cdot x^b$$

$\mathbb{B} = \mathbb{A} \cdot T_{A \rightarrow B}$ – определение матрицы перехода в матричной форме

$\mathbb{A} \cdot x^a = \mathbb{A} \cdot T_{A \rightarrow B} \cdot x^b \Rightarrow$ так как разложение по базису единственно, то $x^a = T_{A \rightarrow B} x^b$

■

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

Пусть U – матрица перехода от базиса e к базису f . Пусть B_e – матрица билинейной формы в базисе e , B_f – матрица билинейной формы в базисе f . Тогда: $B_f = U^T B_e U$

□

$$b(x, y) = (x^e)^T B_e y_e = (U x^f)^T B_e (U y^f) = (x^f)^T \underbrace{U^T B_e U}_{B_f} y^f = (x^f)^T B_f y^f \text{ (где } x^e \text{ – столбец координат}$$

x в базисе e)

$\Rightarrow B_f = U^T B_e U$ (подставляем все базисные векторы)

■

17. Выпишите формулу для преобразования матрицы линейного отображения при замене базиса и докажите её.

Пусть φ – линейное отображение из линейного пространства V_1 в линейное пространство V_2 . Пусть $A_{E_1 E_2}$ – матрица линейного отображения в паре базисов: E_1 в пространстве V_1 и E_2 в пространстве V_2 и пусть T_1 – матрица перехода от E_1 к E'_1 , T_2 – матрица перехода от E_2 к E'_2 . Тогда $A_{E'_1 E'_2} = T_2^{-1} A_{E_1 E_2} T_1$

□

$$X^{E'_1} = T_1^{-1} x^{E_1}; Y^{E'_2} = T_2^{-1} x^{E_2}$$

Пусть y – образ x под действием φ . Тогда

$$Y^{E_2} = A_{E_1 E_2} X^{E_1} \text{ и } Y^{E'_2} = A_{E'_1 E'_2} X^{E'_1} \Rightarrow T_2^{-1} Y^{E_2} = A_{E'_1 E'_2} T_1^{-1} X^{E_1} \Rightarrow Y^{E_2} = \underbrace{T_2 A_{E'_1 E'_2} T_1^{-1}}_{A_{E_1 E_2}} X^{E_1} \Rightarrow$$

$$\Rightarrow A_{E_1 E_2} = T_2 A_{E'_1 E'_2} T_1^{-1}$$

■