Алгебра и теория чисел

Дыбкова Е. В.

I курс, I семестр, 2004 год

Глава 1.

§1.1. Множества, отношения, отображения

Определение 1. *Множество* — совокупность элементов определённой природы.

Примеры: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{R}_+ = \{a \in \mathbb{R} | a > 0\}$, $\mathbb{N}_0 = \{a \in \mathbb{Z} | a \geqslant 0\}$

$|M|$ - число элементов множества M.

Если M_1 и M_2 — множества, то:

- $M_1 \cup M_2 = \{a | a \in M_1 \vee a \in M_2\}$
- $M_1 \cap M_2 = \{a | a \in M_1 \wedge a \in M_2\}$

Если $\forall a \in M_1 \Rightarrow a \in M_2$, то $M_1 \subseteqq M_2$ и говорят, что M_1 является *подмножеством* M_2.

$M_1 \subseteqq M_2$ и $M_2 \subseteqq M_1 \Rightarrow M_1 = M_2$ и говорят, что M_1 и M_2 равны.

$\varnothing \subseteqq M$ для любого множества M.

Если M — конечное множество, то число всех его подмножеств равно $2^{|M|}$

2^M — множество всех подмножеств множества M.

$M_1 \cap M_2 \subseteqq M_1, M_2$; $M_1, M_2 \subseteqq M_1 \cup M_2$

Если M_1, M_2 — множества: $M_1 \setminus M_2 = \{a \in M_1 | a \notin M_2\} \subseteqq M_1$ — *разность* множеств M_1 и M_2.

Если $M_1, M_2 \neq \varnothing$, то $M_1 \times M_2 = \{(a, b) | a \in M_1, b \in M_2\}$ — *декартово произведение*.

Если M_1, M_2 конечны, то $|M_1 \times M_2| = |M_1| \times |M_2|$.

Если $M \neq \varnothing$, то $M \times M = M^2$ — декартов квадрат.

Если $M_1, M_2, \ldots, M_n$ — множества, то

$$M_1 \cup M_2 \cup \ldots \cup M_n = \bigcup_{i=1}^{n} (M_1 \cup \ldots \cup M_{n-1}) \cup M_n$$

$$M_1 \cap M_2 \cap \ldots \cap M_n = \bigcap_{i=1}^{n} (M_1 \cap \ldots \cap M_{n-1}) \cap M_n$$

Если $M_1, M_2, \ldots, M_n \neq \varnothing$, то $M_1 \times M_2 \times \ldots \times M_n = (M_1 \times \ldots \times M_{n-1}) \times M_n$

Определение 2. Пусть $M_1, M_2 \neq \varnothing$. *Бинарным отношением из* M_1 *в* M_2 называется (M_1, M_2, Ω), $\Omega \subseteqq M_1 \times M_2$, Ω — график бинарного отношения.

Примеры:

1. $M = M_1 = M_2 = \mathbb{Z}$, Ω — диагональ декартова квадрата — отношение равенства
2. $M_1 = M_2 = \mathbb{R}$, $(a, b) \in \Omega \Leftrightarrow a > b$

Пусть дано отношение (M, M, Ω). $(a, b) \in \Omega \Leftrightarrow a \omega b$

Определение 3. *Тернарное отношение* (M_1, M_2, M_3, Ω), $\Omega \subseteqq M_1 \times M_2 \times M_3$.

Пример. $M_1 = \mathbb{N}, M_2 = \mathbb{Z}, M_3 = \mathbb{R}$, $(a, b, c) \in \Omega \Leftrightarrow a^b = c$

Определение 4. Пусть (M_1, M_2, Ω) — бинарное отношение из M_1 в M_2. Это бинарное отношение называется отображением из M_1 в M_2 (с началом в M_1 и концом M_2), если выполняется условие:

$$\forall a \in M_1 \quad \exists! \quad b \in M_2 : (a, b) \in \Omega$$

Обозначение: $f : M_1 \to M_2$

$a \in M_1, b \in M_2, (a, b) \in \Omega \Rightarrow$ будем писать, что $b = f(a)$

b называется образом a относительно f, a называется прообразом b относительно f

$\forall b_2 \in M_2$ рассмотрим $\{a \in M_1 | b = f(a)\} \subseteqq M_1$. Это множество называется полным прообразом элемента b и обозначается $f^{-1}(b)$.

Определение 5. Рассмотрим два отображения (M_1, M_2, Ω) и (M_1', M_2', Ω'). Они называются равными тогда и только тогда, когда $M_1 = M_1', M_2 = M_2', \Omega = \Omega'$.

Определение 6. $f : M_1 \to M_2, \quad f_1 : N_1 \to M_2, \quad \varnothing \neq N_1 \subseteqq M_1, \quad f_1(a) = f(a) \quad \forall a \in N_1$. Тогда f_1 называется *ограничением* f на N_1.

Определение 7. Пусть $N_2 \subseteqq M_2$ и $\forall a \in M_1 \quad f(a) \in N_2$. Тогда можно определить $f_2 : M_1 \to M_2 \quad (f_2(a) = f(a) \quad \forall a \in M_1)$. Тогда f_2 называется *срезкой* f на N_2.

Определение 8. $\varnothing \neq N_1 \subseteqq M_1, \quad N_2 \lneqq M_2 : f(a) \in N_2 \quad \forall a \in N_1$. $f_3 : N_1 \to N_2, \quad f_3(a) = f(a) \quad \forall a \in N_1$. Тогда f_3 называется сужением f на N_1.

Определение 9. $\varnothing \neq N_1 \subseteqq M_1, \quad f : M_1 \to M_2$. $f(N_1) = \{f(a) | a \in N_1\} \subseteqq M_2$ называется образом N_1.

Определение 10. Пусть $N_2 \subseteqq M_2$. Тогда полным прообразом N_1 называется $f^{-1}(N_2) = \{a \in M_1 | f(a) \in N_2\} \subseteqq M_1$.

Определение 11. Пусть $f : M_1 \to M_2$.

f называется *инъективным (инъекция, вложение)*, если $\forall a_1, a_2 \in M_1 | a_1 \neq a_2 \; f(a_1) \neq f(a_2)$.

f называется *сюръективным (сюръекция, отображение на)*, если $\forall b \in M_2 \quad \exists a \in M_1 | f(a) = b$.

f называется *биективным (биекция)*, если f является инъекцией и сюръекцией.

Примеры: $M_1 = M_2 = \mathbb{R}, \quad f_1 : \mathbb{R} \to \mathbb{R}$

$f_1(a) = 2^a$ — инъекция, не сюръекция

$f_2(a) = a^3 - a$ — сюръекция, не инъекция

$f_3(a) = a + 1$ — биекция

Определение 12. M — непустое множество, $M_1 \overset{a \mapsto a}{\to} M_2$ — *тождественное отображение*

Обозначение: ε_M

Определение 13. Пусть f_1, f_2 — отображения, $f_2 : M_1 \to M_2, f_1 : M_2 \to M_3$. Тогда *композицией (произведением, суперпозицией)* f_1 и f_2 называется $f_1 \circ f_2 : M_1 \to M_3$: $\forall a \in M_1 (f_1 \circ f_2)(a) = f_1(f_2(a))$

Пусть $f : M_1 \to M_2$, тогда $f \circ \varepsilon_{M_1} = \varepsilon_{M_2} \circ f = f$

$\forall a \in M_1 (f \circ \varepsilon_{M_1})(a) = f(\varepsilon_{M_1}(a)) = f(a)$

Предложение 1. Ассоциативность композиции отображений.

Пусть

$$f_1 : M_1 \to M_2$$

$$f_2 : M_2 \to M_3$$

$$f_3 : M_3 \to M_4$$

Тогда $f_3 \circ (f_2 \circ f_1) = (f_3 \circ f_2) \circ f_1$.

Доказательство. $\forall a \in M_1 f_3 \circ (f_2 \circ f_1)(a) = f_3(f_2 \circ f_1(a)) = f_3(f_2(f_1))(a)$

Пример. Рассмотрим случай: $f_1 : M_1 \to M_2, f_2 : M_2 \to M_3, M_3 = M_2 = M_1 = \mathbb{R}$. $f_1(a) = 2^a, f_2(a) = \sin a$. Докажем, что $f_2 \circ f_1 \neq f_1 \circ f_2$.

$(f_1 \circ f_2)(0) = f_1(\sin 0) = 2^0 = 1$

$(f_2 \circ f_1)(0) = \sin(2^0) = \sin 1 \neq 1$

Определение 14. $f_1 : M_1 \to M_2; f_2 : M_2 \to M_1$. $f_1 \circ f_2 : M_2 \to M_2$. Если $f_1 \circ f_2 = \varepsilon_{M_2}$, то f_1 называется *левым обратным* к f_2, а f_2 — *правым обратным* к f_1.

Пример. $M_1 = \mathbb{R} \setminus \{0\}, M_2 = \mathbb{R}$

$f_1 : M_1 \to M_2, f_1(a) = \log_2(|a|)$

$f_2 : M_2 \to M_1, f_2(a) = 2^a$

$(f_1 \circ f_2)(a) = \log_2(|2^a|) = a = \varepsilon_{M_2}(a)$

$(f_2 \circ f_1)(-2) = 2^{\log_2(|-2|)} = 2 \neq \varepsilon_{M_1}(-2) = -2$

Определение 15. Если $f_1 : M_1 \to M_2; f_2 : M_2 \to M_1$, причём f_1 является одновременно и левым и правым обратным к f_2, то f_1 называется *двусторонним обратным* к f_2.

Определение 16. Если к отображению существует обратное, то оно называется *обратимым*.

Предложение 2. $f : M_1 \to M_2$, g — левое обратное к f, а h — правое обратное к f, то $g = h$.

Доказательство.
$g : M_2 \to M_1$
$h : M_2 \to M_1$
$g \circ f = \varepsilon_{M_1}; f \circ h = \varepsilon_{M_2}$
$h = \varepsilon_{M_1} = (g \circ f) \circ h = g \circ (f \circ h) = g \circ \varepsilon_{M_2} = g$
Следствие 1. Если отображение обратимо, то обратное к нему отображение единственно.
Замечание 1. f обратимо, f^{-1} — обратное к f. Тогда отображение f^{-1} тоже обратимо.
Доказательство. $f : M \to N, f^{-1} : N \to M, f^{-1} \circ f = \varepsilon_M, f \circ f^{-1} = \varepsilon_N$.
Замечание 2. f, g - обратимы, причём определено $f \circ g$. Тогда $f \circ g$ обратимо, причём $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.
Предложение 3. $f : M \to N$. f обратимо $\Leftrightarrow$ f — биекция.
Доказательство.
$\Rightarrow$: $a_1, a_2 \in M$, причём $a_1 \neq a_2$. Пусть $f(a_1) = f(a_2)$. $a_1 = (f^{-1} \circ f)(a_1) = f^{-1}(f(a_1)) = f^{-1}(f(a_2)) = (f^{-1} \circ f)(a_2) = a_2$. Таким образом, f инъективно.

$\forall b \in N f^{-1}(b) = a \in M$. $f(a) = (f \circ f^{-1})(b) = b$. Таким образом, f сюръективно, т. е. f — биекция.
$\Leftarrow$: $\forall b \in N \quad \exists! a \in M : b = f(a)$. $g : N \to M : g(b) = a$. $f^{-1} = g$.
Определение 17. $M \neq \varnothing, I \neq \varnothing, (I, M, \Omega)$ — отображение. Ω — *семейство* в M с индексмножеством I.
Обозначение: $i \in I, x \in M, (i, x) = x_i$; $(x_i)_{i \in I}$
Определение 18. $J \subsetneqq I \Rightarrow (x_i)_{i \in J}$ — подсемейство.
Определение 19. $M \neq \varnothing, (M_i)_{i \in I}$ — непустое семейство в 2^M.

$$\bigcup_{i \in I} M_i = \{x \in M | \exists i \in I : x \in M_i\}$$

$$\bigcap_{i \in I} M_i = \{x \in M | \forall i \in I : x \in M_i\}$$

Определение 20. $(M_i)_{i \in I}$ — непустое семейство непустых подмножеств в M — *разбиение* M, если:

1. $M = \bigcup\limits_{i \in I} M_i$
2. $M_i \cap M_j = \varnothing \quad \forall i, j \in I | i \neq j$

Пример. $M = \mathbb{Z}$ $(\mathbb{N}, 0, \{a \in \mathbb{Z} | a < 0\})$
Определение 21. $a, b \in M$. $a \omega b \Leftrightarrow \exists i \in I : a, b \in M_i$. Таким образом, мы получили бинарное отношение.

1. $\forall a \in M \quad a \omega a$ (рефлексивность)
2. $\forall a, b \in M \quad a \omega b \Rightarrow b \omega a$ (симметричность)
3. $\forall a, b, c \in M \quad \left\{ \begin{array}{l} a \omega b \\ b \omega a \end{array} \right. \Rightarrow a \omega c$ (транзитивность)

В алгебре бинарные отношения, обладающие этими тремя свойствами, принято называть *эквивалентностя*
Примеры:
Пример 1. M, Ω — диагональ M^2. ω — равенство.
Пример 2. $M, \Omega = M^2$. M — тривиальное
Пример 3. $M = \mathbb{Z}$
Определение 22. $M, \sim$ — эквивалентность. $a \in M, \overline{a} = \{b \in M | b \sim a\}$ — *класс эквивалентности* с представителем a.
Определение 23. Множество классов эквивалентности $M/_\sim$ называется *факторомножеством* множества M по эквивалентности $\sim$.
Свойства:

1. $\overline{a} \in M/_{\mathrm{N}} \Rightarrow \overline{a} \neq \varnothing$
2. $b, c \in \overline{a} \Rightarrow b \sim c$
3. $M = \bigcup\limits_{\overline{a} \in M/N}$

4. $b \in \overline{a} \Rightarrow \overline{a} = \overline{b} (c \in \overline{a} \Leftrightarrow b \sim c \Leftrightarrow c \in \overline{b})$

5. $\overline{a}, \overline{b} \in M/_N, \overline{a} \neq \overline{b} \Rightarrow \overline{a} \cap \overline{b} = \varnothing$ $(c \in \overline{a} \cup \overline{b} \Rightarrow c \sim a, c \sim b \Rightarrow a \cap b \Rightarrow \overline{a} = \overline{b}?!)$

$\{$Множество всех разбиений $M\} \leftrightarrows \{$ множество всех эквивалентностей на $M\}$

§1.2. Основные алгебраические структуры

Определение 1. $M_1, M_2, M_3 \neq \varnothing, \varnothing \neq N \subseteq M_1 \times M_2, f : N \to M_3$. $f(a_1, a_2) = a_1 * a_2$
(M_1, M_2, M_3, N, f) называется *бинарным алгебраическим действием.*
Если $N = M_1 \times M_2$, то оно называется *всюду определённым* алгебраическим действием.
$M_1 = M_2 = M_3$ — внутреннее действие
$M_1 = M_3 \neq M_2$ или $M_2 = M_3 \neq M_1$ — внешнее
Примеры:
Пример 1. $M_1 = M_2 = M_3 = \mathbb{N}, N = \mathbb{N}^2, (a, b) \mapsto a + b$ — всюду определённое внутреннее бинарное алгебраическое действие
Пример 2. $M_1 = M_2 = \mathbb{N}, M_3 = \mathbb{Q}, N = \mathbb{N}^2, (a, b) \mapsto \frac{a}{b}$ — всюду определённое бинарное алгебраическое действие
Определение 2. $M, *$ — бинарная операция. $*$ называется *ассоциативной* бинарной операцией, если $\forall a, b, c \in M \quad (a * b) * c = a * (b * c)$. В этом случае M называется *полугруппой*
Определение 3. Пусть $e \in M$. e называется *правым нейтральным элементом* относительно $*$, если $\forall a \in M \quad a * e = a$.
e называется *левым нейтральным элементом* относительно $*$, если $\forall a \in M \quad e * a = a$.
e называется *двухсторонне-нейтральным элементом* относительно $*$, если он левый и правый нейтральный.
Предложение 1. Если e — правый нейтральный элемент относительно $*$, f — левый нейтральный элемент относительно $*$, то $e = f$.
Доказательство. $e = f * e = f$
Определение 4. Полугруппа, в которой существует нейтральный элемент, называется *моноидом.*
Определение 5. $\mathbb{N}_0$ — моноид относительно сложения.
Определение 6. M относительно $*$ — моноид, $a \in M$.
a называется *обратимым справа*, если $\exists a' \in M : a * a' = e$
a называется *обратимым слева*, если $\exists a' \in M : a' * a = e$
a называется *обратимым*, если $\exists a' \in M : a * a' = a' * a = e$
Определение 7. Если в моноиде каждый элемент обратим, то такой моноид называется *группой.*
Пример. $\mathbb{Z}, +$
Замечание 1.

Мультипликативная терминология:

- операция — умножение,
- нейтральный элемент — 1,
- обратный элемент — a^{-1}

Аддитивная терминология:

- операция — сложение,
- нейтральный элемент — 0,
- обратный элемент — $-a$

Определение 8. $*$ называется *коммутативной* операцией в M, если $\forall a, b \in M \quad a * b = b * a$.
Определение 9. Если M — группа относительно $*$ и $*$ коммутативна, то M называется *коммутативной* или *абелевой* группой.
Примеры:
Пример 1. $\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+, (2\mathbb{Z})^+$
Пример 2. $\mathbb{Q}^* = \{\alpha \in \mathbb{Q} | \alpha \neq 0\}$,
$\mathbb{R}^* = \{\beta \in \mathbb{R} | \beta \neq 0\}$,
$\mathbb{Q}_+^*, \mathbb{R}_+^*, \{\pm 1\}$ (все эти группы абелевы)

Пример 3. $\{a\} = M, a * a = a$ — эта группа называется *единичной* группой.
Пример 4. M — непустое множество, $S(M) = \{f : M \to M$ — биекция $\}$
Предложение 2. Если M содержит больше двух элементов, то $S(M)$ — неабелева группа.
Доказательство. a_1, a_2, a_3 — различные элементы в M. $f_1, f_2 : M \to M$.

$$f_1(a) = \begin{cases} a, & \text{если } a \neq a_1, a_2 \\ a_2, & \text{если } a = a_1 \\ a_1, & \text{если } a = a_2 \end{cases}$$

$$f_2(a) = \begin{cases} a, & \text{если } a \neq a_1, a_3 \\ a_3, & \text{если } a = a_1 \\ a_1, & \text{если } a = a_3 \end{cases}$$

$f_1, f_2 \in S(M)$
$(f_1 \circ f_2)(a_1) = f_1(f_2(a_1)) = f_1(a_3) = a_3$
$(f_2 \circ f_1)(a_1) = f_2(f_1(a_1)) = f_2(a_2) = a_2, a_3 \neq a_2 \Rightarrow$
$f_1 \circ f_2 \neq f_2 \circ f_1$.
Предложение 3. Пусть M — группа относительно $*$, e — нейтральный элемент. Тогда:

1. обратный к любому элементу группы определён однозначно
2. если $a \in M$ и a' — обратный к a, то $(a')' = a$
3. если $a, b \in M$, то $(a * b)' = b' * a'$

Определение 10. $\forall n \in \mathbb{Z}, \forall a \in G$

$$a^n = \begin{cases} \underbrace{a \dots a}_{n} & , \quad n \in \mathbb{N} \\ 1 & , \quad n = 0 \\ (a^{-1})^{-n} & , \quad n < 0 \end{cases}$$

Утверждение 1. $\forall m, n \in \mathbb{Z} \quad a^{m+n} = a^m a^n$
(но $(ab)^n$ не всегда совпадает с $a^n b^n$)
Определение 11. G — аддитивно заданная группа. $\forall n \in \mathbb{Z}, \forall a \in G$

$$na = \begin{cases} \underbrace{a + a + \ldots + a}_{n} & , \quad n \in \mathbb{N} \\ 1 & , \quad n = 0 \\ \underbrace{(-a) + \ldots + (-a)}_{-n} & , \quad n < 0 \end{cases}$$

Определение 12. G — группа, $H \subseteqq G$. H называется подгруппой группы $G (H \leqslant G)$, если H — тоже группа относительно той же операции, что и G.
Пример. $\mathbb{Z} \leqslant \mathbb{Q}^+$
Предложение 4. G — группа, $H \leqslant G \Rightarrow$

1. $1_H = 1_G$
2. если $a \in H$, то обратный к a в H совпадает с обратным к a в G.

Доказательство.

1. $1_H \cdot 1_H = 1_H, 1_H^{-1} \in G$
   $1_H = 1_G \cdot 1_H = (1_H^{-1} \cdot 1_H) \cdot 1_H = 1_H^{-1} \cdot (1_H \cdot 1_H) = 1_H^{-1} \cdot 1_H = 1_G$
2. Если a^{-1} — обратный к a в G, $\hat{a}$ — обратный к a в H, то $\hat{a}a = a\hat{a} = 1_H = 1_G \Rightarrow \hat{a}$ — обратный к a в $G \Rightarrow \hat{a} = a^{-1}$

Теорема 1. *Критерий подгруппы*
G — группа, $H \subseteqq G$. Тогда $H \leqslant G \Leftrightarrow$

1. $H \neq \varnothing$
2. если $a, b \in H$, то $ab \in H$ (замкнутость H относительно бинарной операции)
3. если $a \in H$, то $a^{-1} \in H$ (замкнутость H относительно обращения элементов)

Доказательство. $\Rightarrow$: Докажем, что в H есть нейтральный элемент, т. е. $1_G \in H$. (1) $\exists a \in H \overset{3}{\Rightarrow} a^{-1} \in H \overset{2}{\Rightarrow} a \cdot a^{-1} = 1_G \in H$

Утверждение 2. Свойство быть подгруппой является транзитивным бинарным отношением

Доказательство. $F \leqslant H \leqslant G$, причём $f \leqslant H, H \leqslant G \Rightarrow F \leqslant G$

Примеры:

Пример 1. $2\mathbb{Z} \leqslant \mathbb{Z} \leqslant \mathbb{R}^+$

Пример 2. $\mathbb{Q}^+ \leqslant \mathbb{R}^*, \mathbb{Q}_+^* \leqslant \mathbb{Q}^*, \{\pm 1\} \leqslant \mathbb{R}^+$

Пример 3. $\mathbb{Q}_+^* \subsetneqq \mathbb{Q}_+$, однако $\mathbb{Q}_+^* \not\leqslant \mathbb{Q}_+$

Пример 4. G — любая группа, $\{1\}, G \leqslant G$ (*тривиальные* подгруппы G)

Определение 13. Пусть K — множество с двумя бинарными операциями $+$ и $-$. K называется *кольцом* относительно этих двух операций, если:

1. $(a + b) + c = a + (b + c) \quad \forall a, b, c \in K$
2. $\exists$ "0" $\in K : 0 + a = a + 0 = a \quad \forall a \in K$
3. $\forall a \in K \; \exists$ "$-a$" $\in K : a + (-a) = (-a) + a = 0$
4. $\forall a, b \in K \quad a + b = b + a$
5. $a(b + c) = (ab) + (ac) \quad \forall a, b, c \in K$
6. $(a + b)c = ac + bc \quad \forall a, b, c \in k$

Примеры:

Пример 1. $\mathbb{Z}(+, \cdot)$

Пример 2. $\mathbb{Z}(+, ab = 0 \quad \forall a, b)$

Пример 3. $2\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ — кольца относительно $+$ и $\cdot$

Пример 4. $\{a\}$ — нулевое кольцо

Пример 5. $K = \{f : \mathbb{R} \to \mathbb{R}\}, \quad \forall f_1, f_2 \in K, \quad \forall \alpha \in \mathbb{R}$
$(f_1 + f_2)(\alpha) = f_1(\alpha) + f_2(\alpha)$
$(f_1 \cdot f_2)(\alpha) = f_1(\alpha) \cdot f_2(\alpha)$

Определение 14. Для любого кольца K мы можем определить операцию вычитания как $a - b = a + (-b)$

Определение 15. $(a_i)_{i \in \Omega} \quad (\Omega$ – бесконечное) — почти конечное, если $\exists$ конечное $J \subsetneqq \Omega | a_i = 0 \quad \forall i \in \Omega \setminus J \quad \sum\limits_{i \in \Omega} \sum\limits_{i \in J} a_i$

Предложение 5. K — кольцо $\Rightarrow$

1. $a \cdot 0 = 0 \cdot a \quad \forall a \in K$
2. $(-a) \cdot b = a \cdot (-b) = -ab \quad \forall a, b \in K$
3. $(a - b) \cdot c = ac - bc, a(b - c) = ab - ac \quad \forall a, b, c \in K$

Доказательство.

1. $a \cdot 0 = a(0 + 0) = a \cdot 0 + a \cdot 0$. Прибавим к обеим частям $-a \cdot 0$. $0 = a \cdot 0 + 0 = a \cdot 0$
2. $(-a) \cdot b + ab = ((-a) + a) \cdot b = 0 \cdot b = 0 \Rightarrow (-a) \cdot b = -ab$

Определение 16. Кольцо K называется *ассоциативным*, если все введённые там операции ассоциативны.
Определение 17. Кольцо K называется *кольцом с единицей*, если K ассоциативно и $\exists 1 \neq 0$.
Определение 18. Кольцо K называется *коммутативным*, если оно ассоциативно и операция умножения коммутативна.
Определение 19. *Телом* называется кольцо с единицей, в котором каждый ненулевой элемент обратим.
Определение 20. *Поле* — коммутативное кольцо.
Утверждение 3. В любом кольце с единицей 0 не обратим.
Определение 21. K — кольцо с единицей. $K^* = \{a \in K | ab = ba = 1$ при некотором $b \in K\}$. K^* называется *группой обратимых элементов* K.
Утверждение 4. Если K — поле, то можно определить деление на ненулевой элемент: $b \neq 0, a : b = a \cdot (b^{-1})$.
Определение 22. K — кольцо, $a \in K, a \neq 0$. a называется *правым нетривиальным делителем* 0, если $\exists b \in K : ba = 0$.

$$f_1(\alpha) = \begin{cases} 1 & , \quad \alpha \geqslant 0 \\ 0 & , \quad \alpha < 0 \end{cases} \quad f_2(\alpha) = \begin{cases} 0 & , \quad \alpha \geqslant 0 \\ 2 & , \quad \alpha < 0 \end{cases}$$

Предложение 6. K — кольцо с единицей, a — нетривиальный правый (левый) делитель $0 \Rightarrow a \notin K^*$
Доказательство. $ab = 0; b \in K, b \neq 0$.
Пусть a обратим и $c = a^{-1}$.
$b = 1 \cdot b = (ca)b = c(ab) = c \cdot 0 = 0$?!
Определение 23. Коммутативное кольцо с 1 называется *областью целостности*, если в нём нет нетривиальных делителей 0.
Определение 24. Пусть K — кольцо, $k \subseteq K$. k называется *подкольцом* кольца K ($k \leqslant K$), если k является кольцом относительно той же операции, что и кольцо k.
Пример. $2\mathbb{Z} \leqslant \mathbb{Z} \leqslant \mathbb{Q} \leqslant \mathbb{Q}$
Теорема 2. Критерий подкольца.
K — кольцо, $k \leqslant K$. Тогда $k \leqslant K \Leftrightarrow$

1. $k \leqslant K^+$
2. $\forall \alpha, \beta \in K \quad \alpha\beta \in K$ (замкнутость относительно умножения)

Определение 25. Пусть K — ассоциативное кольцо. Тогда $\mathfrak{A} \subseteq K$ — идеал кольца K, если

1. $\mathfrak{A} \leqslant K^+$
2. $\forall a \in \mathfrak{A} \quad \forall \alpha \in K \quad \alpha a, a\alpha \in \mathfrak{A}$

Обозначение: $\mathfrak{A} \trianglelefteq K$
Примеры:
Пример 1. $2\mathbb{Z} \trianglelefteq \mathbb{Z}$
Пример 2. $\mathbb{Z} \leqslant \mathbb{Q}$, но $\mathbb{Z} \not\trianglelefteq \mathbb{Q} \quad (\frac{1}{3} \cdot 2 \notin \mathbb{Z})$
Пример 3. $\left.\begin{matrix} \{0\} \trianglelefteq K \\ K \trianglelefteq K \end{matrix}\right\}$ тривиальные кольца
Пример 4. K — коммутативное кольцо, $a \in K \quad \{\alpha a | \alpha \in K\}$. Если K — кольцо с 1, то $a \in \{\alpha a | \alpha \in K\} = <a>$ — *главный идеал* кольца K, порождённый элементом a.
$\{0\} = <0>$
$K = <1>$
Предложение 7. Если K — некоторое тело, то все его идеалы тривиальны.
Доказательство. $\mathfrak{A} \trianglelefteq K, \mathfrak{A} \neq \{0\}$
$a \in \mathfrak{A}, a \neq 0. \quad \exists a^{-1} \in K : a^{-1} \cdot a = 1 \in \mathfrak{A} \quad \forall b \in K, b = b \cdot 1 \in \mathfrak{A}$. $K \subseteq \mathfrak{A} \Rightarrow \mathfrak{A} = K$.
Определение 26. K — кольцо главных идеалов (КГИ), если

1. K — область целостности (коммутативное кольцо с 1, где нет нетривиальных делителей 0).
2. Любой идеал K — главный идеал

K — ассоциативное кольцо, $\mathfrak{A} \trianglelefteq K$. $(a,b) \in \mathfrak{A} \Leftrightarrow a-b \in \mathfrak{A}$
$(a,b),(b,c) \in \mathfrak{A} \Rightarrow (a,c) \in \mathfrak{A} \quad (a-b, b-c \in \mathfrak{A} \Rightarrow a-c \in \mathfrak{A})$
$a \sim b, K/\tilde{\mathfrak{A}}$
Определение 27. Пусть имеется два класса $\overline{a}, \overline{b} \in K/\mathfrak{A}$
$\overline{a} + \overline{b} = \overline{a+b}$
$\overline{a} \cdot \overline{b} = \overline{ab}$
Корректность. $a_1 \sim a, b_1 \sim b$
$$ab - a_1b_1 = ab - ab_1 + ab_1 - a_1b_1 = \underbrace{a\underbrace{(b-b_1)}_{\in \mathfrak{A}}}_{\in \mathfrak{A}} + \underbrace{\underbrace{(a-a_1)}_{\in \mathfrak{A}} b_1}_{\in \mathfrak{A}} \in \mathfrak{A}$$
$ab \sim a_1b_1$
$\overline{ab} = \overline{a_1b_1}$
Предложение 8. Относительно введённых операций $K/\mathfrak{A}$ — ассоциативное кольцо.
Доказательство. $\overline{0} = \mathfrak{A}, \quad \forall \overline{a} \in K/\mathfrak{A} \quad \overline{a} + \overline{0} = \overline{a+0} = \overline{a} = \overline{0+a} = \overline{0} + \overline{a} \Rightarrow \overline{0}$ — нейтральный элемент относительно $+$ в $K/\mathfrak{A}$.
Определение 28. Полученное кольцо $K/\mathfrak{A}$ называется *факторкольцом* кольца K по его идеалу $\mathfrak{A}$.
Предложение 9. K — ассоциативное кольцо, $\mathfrak{A} \trianglelefteq K \Rightarrow$

1. $\mathfrak{A} = K \Leftrightarrow K/\mathfrak{A}$ — нулевое кольцо
2. если K — коммутативное, то $K/\mathfrak{A}$ — тоже коммутативное
3. если K — кольцо с 1 и $\mathfrak{A} \neq K$, то $K/\mathfrak{A}$ — тоже кольцо с 1.

Доказательство. 1. $\Leftarrow K/\mathfrak{A}$ состоит из одного элемента, значит в K всего один класс эквивалентности.
Определение 29. K — кольцо с 1, M — непустое множество. M — *левый K-модуль*, если определены 2 действия — бинарная операция на M $(+)$ и внешнее всюду определённое действие $K \times M \to M$ (умножение на скаляры из кольца K), причём

1.
2.
3.
4. M^+ — абелева группа
5. $(\alpha+\beta)a = \alpha a + \beta a \quad \forall \alpha, \beta \in K, \quad \forall a \in M$
6. $\alpha(a+b) = \alpha a + \alpha b \quad \forall \alpha \in K, \quad \forall a, b \in M$
7. $\alpha(\beta a) = (\alpha\beta)a \quad \forall \alpha, \beta \in K, \quad \forall a \in M$
8. $1 \cdot a = a \quad \forall a \in M$ — унитальность

Примеры:
Пример 1. K — ассоциативное кольцо с 1, $n \in \mathbb{N}$
$M = \{(\alpha_1, \dots, \alpha_N) | \alpha_i \in K\}$
$(\alpha_1, \dots, \alpha_n) + (\beta_1, \dots, \beta_n) = (\alpha_1 + \beta_1, \dots, \alpha_n + \beta_n)$
$\beta(\alpha_1, \dots, \alpha_n) = (\beta\alpha_1, \dots, \beta\alpha_n)$
M — левый K-модуль
Пример 2. G^+ — абелева группа. $\quad \forall a \in G \quad \forall m \in \mathbb{Z} \quad \mathbb{Z} \times G \to G \quad m \cdot a = ma$
Определение 30. Если K — поле, то левый K-модуль называется *линейным (векторным) пространством* над K.
Определение 31. K — поле, A — линейное пространство над K. Если в A определена ещё одна бинарная операция (умножение), то A называется *алгеброй* над K, когда выполнены следующие требования:

1. $A(+,\cdot)$ — кольцо

2. $(\alpha a)b = a(\alpha b) \quad \forall \alpha \in K, \quad \forall a, b \in A$

Пример. $K = \mathbb{Q}, A = \mathbb{R}$. $\mathbb{R}$ — алгебра над $\mathbb{Q}$.

Определение 32. G_1, G_2^* — две группы. $G_1 \cong G_2^*$ (G_1 *изоморфно* G_2), если существует такая биекция $f : G_1 \to G_2$, что $f(a \cdot b) = f(a) * f(b)$.

(Биекция f, удовлетворяющая указанному свойству, называется *изоморфизмом групп*).

Предложение 10. Изоморфность является эквивалентностью на множестве всех групп.

Доказательство.

1. **Рефлексивность.**

$\varepsilon_G : G \to G$ — изоморфизм групп. $\varepsilon_G(a, b) = ab = \varepsilon_G(a) \cdot \varepsilon_G(b)$

2. **Симметричность.**

$G_1^\cdot \cong G_2^*$. $\exists f : G_1 \to G_2$ — изоморфизм групп. $\exists f^{-1} : G_2 \to G_1$. Осталось доказать, что $f^{-1}(\alpha * \beta) = f^{-1} \cdot f^{-1}(\beta) \quad \forall \alpha, \beta \in G_2$.

$f(f^{-1}(\alpha * \beta)) = \underbrace{(f \circ f^{-1})}_{\varepsilon_{G_2}}(\alpha * \beta) = \alpha * \beta.$

$f(f^{-1}(\alpha) \cdot f^{-1}(\beta)) = f(f^{-1}(\alpha)) * f(f^{-1}(\beta)) = \alpha * \beta$

Поскольку образы одинаковы, а f — инъекция, то и прообразы одинаковы. Тогда f^{-1} — изоморфизм групп $\Rightarrow G_2^* \cong G_1^\cdot$.

3. **Транзитивность.**

$f : G_1^\cdot \to G_2^*$ — изоморфизм групп

$g : G_2^\cdot \to G_3^\circ$ — изоморфизм групп

$g \circ f : G_1^\cdot \to G_3^\circ$ — биекция

$(g \circ f)(a_1 \cdot a_2) = (g \circ f)(a_1) \circ (g \circ f)(a_2) \quad \forall a_1, a_2 \in G_1$

Предложение 11. $f : G_1^\cdot \to G_2^*$ — изоморфизм групп. Если G_1 — абелева, то G_2 — тоже абелева.

Доказательство. $\forall \alpha, \beta \in G_2 \ \exists a, b \in G_1 : \alpha = f(a), \beta = f(b)$. $\alpha * \beta = f(a) * f(b) = f(ab) = f(ba) = f(b) * f(a) = \beta * \alpha$

Определение 33. K_1, K_2 — кольца, $K_1 \cong K_2$, если существует биекция $f : K_1 \to K_2$, согласованная со всеми операциями кольца.

$$\left.\begin{array}{rcl} f(a+b) & = & f(a) + f(b) \\ f(\alpha a) & = & \alpha f(a) \end{array}\right\} \forall a, b \in M, \quad \forall \alpha \in K$$

Определение 34. A_1, A_2 — две алгебры над полем K. $A_1 \cong A_2$, если существует биекция $f : A_1 \to A_2$, которая является изоморфизмом линейных пространств и изоморфизмом колец, т.е. биекция согласована со всеми тремя операциями в алгебре.

Замечание 1. Изоморфность является эквивалентностью на множестве алгебр над одним и тем же полем.

Глава 2. Целые числа и их родственники.

§2.1. Делимость в кольцах.

Определение 1. K — коммутативное кольцо с 1. $a, b \in K$. $a \vdots b \Leftrightarrow \exists c \in K : a = bc$.

Свойства:

Свойство 1. $a \vdots a \ \forall a$

Свойство 2. $a \vdots b, b \vdots c \Rightarrow a \vdots c$

$(a = ba_1, b = cd \Rightarrow a = ca_1 d \Rightarrow a \vdots c)$

Свойство 3. $a \vdots b \Leftrightarrow < a > \subseteq < b >$

$a = bc \in < b > \quad \forall t \in < a > \ t = a \cdot c_1 = bcc_1 \in < b >$

Свойство 4. $a, b \vdots c \Rightarrow a \pm b \vdots c$

Свойство 5. $a \vdots b, c \vdots d \Rightarrow ac \vdots bd$

Свойство 6. $0 \vdots a \ \forall a \in K$

Определение 2. Пусть K — область целостности. a ассоциирован с b, если $a \vdots b, b \vdots a$.

Примечание. Это бинарное отношение является отношением эквивалентности.

Предложение 1. Пусть K — область целостности, $a, b \in K$. Тогда следующие условия эквивалентны.

1. $a \sim b$
2. $<a> = <b>$
3. $\exists \alpha \in K^* : a = b\alpha$

Доказательство.
$1 \Leftrightarrow 2$ следует из определения
$1 \Rightarrow 3$: $a = bc, b = ad$. $a = a \cdot c \cdot d \Rightarrow 0 = a(1 - cd) \Rightarrow \left[\begin{array}{l} a = 0 \\ 1 = cd \end{array}\right.$
$a = 0 \Rightarrow b = 0 \quad a = b = 1a \neq 0 \Rightarrow 1 = cd, c \in K^*$
$3 \Rightarrow 1$: $a = b\alpha, \alpha \in K^*$. $a = 0 \Rightarrow b = 0 \Rightarrow a \sim b$. $a \neq 0 \Rightarrow \exists \beta \in K^* : 1 = \alpha\beta$. $a\beta = b \cdot 1 = b \Rightarrow a \sim b$.
$\{0\} \in K/\sim$; $K^* \in K/\sim$
Если $\{0\}, K^*$ — все классы ассоциированных элементов, то K — поле.

Определение 3. a — *неразложимый* элемент (*простой*), если у него имеются только тривиальные делители.
$a = bc \Rightarrow b \sim a, c \sim 1 \vee b \sim 1, c \sim a$.
В противном случае a — *разложимый*.

Примечание. Элемент, ассоциированный с простым — простой, с разложимым — разложимый.
Пример. $K = \mathbb{Z} : -2$ — простой, 28 — разложимый, -1 не является простым или разложимым.
Определение 4. K — область целостности, $a, b \in K, d \in K$. d — НОД(a, b), если

1. $a \vdots d, b \vdots d$
2. $a \vdots c, b \vdots c \Rightarrow d \vdots c$

Пример. НОД$(0, 0) = 0$
Теорема 1. (о НОД в КГИ)
K — КГИ $\Rightarrow$

1. $\forall a, b \in K \quad \exists$НОД$(a, b)$
2. d — НОД$(a, b), c \in K$. c — НОД$(a, b) \Leftrightarrow c \sim d$
3. d — НОД$(a, b) \Rightarrow \exists u, v \in K : d = au + bv$ (линейное представление НОД)

Доказательство. 1. $\mathfrak{A} = \{ax + by | x, y \in K\}$.$\mathfrak{A} \leqslant K : \mathfrak{A} \neq \varnothing, a, b \in \mathfrak{A}, (ax_1 + by_1) + (ax_2 + by_2) = a(x_1 + x_2) + b(y_1 + y_2)$
$\mathfrak{A} \in K^+$
$\forall c \in K \quad c(ax + by) = a(cx) + b(cy) \in \mathfrak{A}$
$\mathfrak{A}$ — главный идеал кольца $K \Rightarrow \exists d \in$: $\mathfrak{A} = <d>$.$a, b \in <d>, a = da_1, b = db_1$
$\exists x_0, y_0 \in K : d = ax_0 + by_0$.$a \vdots c, b \vdots c \Rightarrow d \vdots c$.
3. Мы доказали в 1), что некоторый НОД(a, b) представляется в указанном виде: d' — некоторый НОД$(a, b), \exists u', v' \in K : d' = au' + bv'$. Пусть d — произвольный НОД$(a, b) \Rightarrow d \sim d', d = d'\alpha, \alpha \in K^*$.

Примечание. В пункте 3 таких пар a и b может быть много.
Определение 5. Два элемента мы будем называть *взаимно простыми*, если 1 — их НОД.
Свойства: (взаимно простых элементов в КГИ)
Свойство 1. $a, b \in K, a$ и b взаимно просты $\Leftrightarrow 1 = au + bv$ для некоторых u и v.
Доказательство. $\Leftarrow$: $a, b \neq 0, d =$ НОД$(a, b) \Rightarrow d \neq 0, a \vdots d, b \vdots d \Rightarrow 1 \vdots d \Rightarrow 1 \sim d, d \in K^*$
Свойство 2. $d \neq 0, d - - -$ НОД$(a, b), a = da_1, b = db_1 \Rightarrow a_1$ и b_1 взаимно просты
Доказательство. $d = au + bv = da_1u + db_1v \Rightarrow 0 = d(1 - a_1u - b_1v) \Rightarrow 1 = a_1u + b_1v \Rightarrow a_1$ и b_1 взаимно просты.
Свойство 3. a_1 и b взаимно просты, a_2 и b взаимно просты $\Rightarrow a_1a_2$ и b взаимно просты.
Доказательство. $\left.\begin{array}{l} 1 = a_1u_1 + bv_1 \\ 1 = a_2u_2 + bv_2 \end{array}\right\} \Rightarrow 1 = a_1a_2u_1u_2 + b(v_1(a_2u_2 + bv_2) + a_1u_1v_2)$
Свойство 3′. $a_1, \ldots, a_n, b \in K$, причём a_i взаимно просто с $b \; \forall i \Rightarrow a_1 \cdot \cdots \cdot a_n$ взаимно просто с b.

Свойство 4. $a_1, a_2 \vdots b$, причём a_1, b взаимно просты $\Rightarrow a_2 \vdots b$

Доказательство. $1 = a_1u + bv, a_2 = (a_1a_2)u + a_2bc \Rightarrow a_2 \vdots b$.

Свойство 5. $a \vdots b_1, b_2$, причём b_1 и b_2 взаимно просты $\Rightarrow a \vdots (b_1b_2)$

Доказательство. $1 = b_1u + b_2v, a = ab_1u + ab_2v \Rightarrow a \vdots b_1b_2$

Свойство 5′. $a, b_1, \ldots, b_n \in K$, причём $a \vdots b_i\ \forall i$ и b_i попарно взаимно просты $\Rightarrow a \vdots b_1 \ldots b_n$

Определение 6. K — ОЦ. K называется *евклидовым кольцом*, если $\exists g : K \setminus \{0\} \to \mathbb{N}_0$, обладающее свойствами:

1. если $a \vdots b (a, b \neq 0)$, то $g(a) \geqslant g(b)$
2. $\forall a, b \in K | b \neq 0\ \exists q, r \in K : a = bq + r$, причём $r = 0 \vee g(r) < g(b)$

(g — *функция порядка*)

Пример. K — поле. $g(a) = 0\ \forall a \neq 0$.
$a = bc. a \neq 0 \Rightarrow a = b(\frac{a}{b}) + a, a = 0 \Rightarrow a = b \cdot 0 + 0$

Теорема 2. (Теорема о делении с остатком для $\mathbb{Z}$)
$\forall a, b \in \mathbb{Z} | b \neq 0\ \exists! q, r \in \mathbb{Z} : a = bq + r$, где $0 \leqslant r < |b|$

Доказательство. $\exists$: достаточно доказать для $b > 0$ (если $b < 0$ и $a = (-b)q + r$ — — — $\exists$ представление, то $a = b(-q) + r$)
$a = 0 : 0 = b \cdot 0 + 0$
$a > 0 : a < b \Rightarrow a = b \cdot 0 + a; a > b \Rightarrow a - b = bq_1 + r_1 \Rightarrow a = b(q_1 + 1) + r_1$
$a < 0 : -a = bq_1 + r_1 \Rightarrow a = b(-q_1) - r_1 \Rightarrow$(если $r_1 \neq 0$)$a = b(-q_1 - 1) + b - r_1$
! : $a = bq_1 + r_1 = bq_2 + r_2$. Если $r_1 = r_2$, то $b(q_1 - q_2) = 0 \Rightarrow q_1 = q_2$. Пусть $r_1 \neq r_2$. $r_1 - r_2 = b(q_2 - q_1) \Rightarrow q_2 \neq q_1$
$|b| > |r_1 - r_2| = |b||q_2 - q_1| \geqslant |b|$

Следствие 1. $\mathbb{Z}$ — ЕК, модуль — функция порядка в этом ЕК.

Предложение 2. Любое евклидово кольцо является кольцом главных идеалов.
$\{0\} \neq \mathfrak{A} \trianglelefteq K (K$ — ЕК$)\ a \in \mathfrak{A}, a \neq 0$. Выберем $b \in \mathfrak{A} | b \neq 0, g(b) \leqslant g(a)\ \forall a \in \mathfrak{A} \setminus \{0\}. <b> = \mathfrak{A}\ \ \forall a \in \mathfrak{A} a = bc, c \in K$
$a \neq 0, a = bc + r$, где $r = 0$ и $g(r) < g(b). r \neq 0\ r \in \mathfrak{A}$?!

Алгоритм Евклида
K — ЕК, $a, b \in K, b \neq 0\ a = bq_1 + r_1, r_1 = 0 \vee g(r_1) < g(b)$
$r_1 \neq 0 \quad b = r_1q_2 + r_2, r_2 = 0 \vee g(r_2) < g(r_1)$
$r_2 \neq 0 \quad r_1 = r_2q_3 + r_3, r_3 = 0 \vee g(r_3) < g(r_2)$
$\vdots$
$r_{k-2} = r_{k-1}q_k + r_k$
$r_{k-1} = r_kq_{k+1} + 0$
$r_k =$ НОД(a, b).

K — ЕК, $a \sim b, g(a) = g(b), a, b \neq 0$

Предложение 3. $a, b \neq 0, a \vdots b, b \not\vdots a \Rightarrow g(a) > g(b)$

Доказательство. т.к. $a \vdots b \Rightarrow g(a) \geqslant g(b) \quad b = aq + r, r \neq 0, g(r) < g(a), r = b - aq, a = bc$, т.е. $r = b(1 - cq) \Longrightarrow r \vdots b \Rightarrow g(a) > g(r) \geqslant g(b)$

Свойства простых элементов в ЕК.

Свойство 1. Если $a \in K, a \neq 0, a \notin K^*$, то $\exists$ простое $p \in K : a \vdots p$

Доказательство. a — либо простой, либо разложимый. Пусть $a = a_1b_1$, где $a_1 \not\sim a, b_1 \not\sim a \Rightarrow g(a_1) < g(a)$. Рассмотрим $a_1 \neq 0, a_1 \in K^+$ (т.к. иначе $b_1 \sim a$) $\Rightarrow a_1$ — либо простой (тогда a_1 — делитель a), либо разложимый. Пусть a_1 — разложимый. Тогда $a_1 = a_2b_2, a_2 \not\sim a_1, b_2 \not\sim a_1, g(a_2) < g(a_1)$. Т.к. $g(a_i) \in \mathbb{Z}$ и $g(a_i)$ убывает, то $\exists a_k = a_{k+1}b_{k+1}, a_{k+1}$ — простой.

Свойство 2. p — простой, $a \in K \Rightarrow a \vdots p \vee a$ и p взаимно просты.

Доказательство. a и p не взаимно просты. $d =$ НОД$(a, p) \Rightarrow d \notin K^*, d \neq 0. p \vdots d \Rightarrow d \sim p. d = p\alpha, \alpha \in K^*. a \vdots d \Rightarrow a \vdots p$

Свойство 3. p_1 и p_2 — два простых элемента $\Rightarrow p_1$ и p_2 взаимно просты $\vee p_1 \sim p_2$.

Доказательство. Если p_1 и p_2 не взаимно просты, то $p_1 \vdots p_2, p_2 \vdots p_1 \Rightarrow p_1 \sim p_2$.

Свойство 4. p — простое, $a_1, a_2 \in K | a_1 a_2 \vdots p \Rightarrow a_1 \vdots p \vee a_2 \vdots p$.

Доказательство. $a_1 \not\vdots p, a_2 \not\vdots p \Rightarrow \left.\begin{array}{c} a_1 \text{ и } p \text{ взаимно просты} \\ a_2 \text{ и } p \text{ взаимно просты} \end{array}\right\} \Rightarrow a_1 a_2$ и p взаимно просты

Замечание 1. В произвольной области целостности любой элемент, обладающий свойством 4, является неразложимым.

Свойство 4′. p — простое, $a_1, \ldots, a_n \in K | a_1 \ldots a_m \vdots p \Rightarrow \exists i | a_i \vdots p$

Свойство 5. $p \neq 0$, p — простое $\Leftrightarrow K/_{<p>}$ — поле.

Доказательство.

$\Rightarrow$: $p \notin K^*, <p> \neq K$. $K/_{<p>}$ не является нулевым кольцом. $K/_{<p>}$ — коммутативное кольцо с 1. $\overline{a} \in K/_{<p>}, \overline{a} \neq \overline{0} \Leftrightarrow a \not\vdots p \Rightarrow a$ и p взаимно просты $\Rightarrow \exists b, c \in K : 1 = ab + pc \Rightarrow \overline{1} = \overline{a} \cdot \overline{b} + \overline{p} \cdot \overline{c} = \overline{a} \cdot \overline{b}$. Следовательно $\overline{a} \in (K/_{<p>})^*$.

$\Leftarrow$: $K/_{<p>}$ — поле. Предположим, что p не является простым. $p \notin K^*, p$ — разложим: $\exists b, c \in K : p = b \cdot c, b, c \not\sim p$. $\overline{0} = \overline{p} = \overline{b} \cdot \overline{c} \Rightarrow \overline{b} = \overline{0} \vee \overline{c} = \overline{0} \quad (b \vdots p \Rightarrow b \sim p ?!) \vee (c \vdots p \Rightarrow c \sim p ?!)$

Теорема 3. (Основная теорема арифметики)

a — любой ненулевой и необратимый элемент ЕК K. Тогда:

1. $a = p_1 \ldots p_s$, где p_i — простые
2. $a = p_1 \ldots p_s = q_1 \ldots q_r$, где p_i и q_j — простые, то $s = r$ и сомножители второго произведения можно поменять местами так, что $p_i \sim q_1 \, \forall i = 1, \ldots, s$

Доказательство. $\exists$: Индукция по $g(a)$.

База: пусть $g(a) \leqslant g(b) \, \forall b \in K | b \neq 0, b \in K^* \Rightarrow a$ — простой (если a — разложимый, то $a = bc, b, c \not\sim a, g(a) > g(b) ?!$).

Пусть $n \in \mathbb{N}$, утверждение 1 справедливо для всех $b | g(b) < n$. $g(a) = n \quad a$ — разложимый $\Rightarrow a = bc, b, c \not\sim a, g(b), g(c) < n$

!: $s \leqslant r . s = 1 \Rightarrow p_1 = q_1 \ldots q_r \Rightarrow \exists i$ (можно считать $i = 1$): $q_i \vdots p_1 \Rightarrow p_1 \vdots q_1$, т.е. $q_1 = p_1 \alpha, \alpha \in K^* . 0 = p_1(1 - \alpha q_2 \ldots q_r) \Rightarrow 1 = \alpha q_2 \ldots q_r \Rightarrow q_r \in K^* ?! \Rightarrow r = 1 = s$

Переход: $\exists i : q_i \vdots p_1, q_i \sim p_1$ (можно считать $i = 1$). $q_1 = p_1 \alpha . p_1 \ldots p_s = \alpha p_1 q_2 \ldots q_r \Rightarrow p_2 \ldots p_s = (\alpha q_2) q_3 \ldots q_r$,

Замечание 1. Кольцо называется факториальным, если это область целостности и для него справедлива основная теорема арифметики, т.е. каждый ненулевой необратимый элемент раскладывается в произведение простых сомножителей, причём разложение однозначно.

§2.2. Целые числа. Сравнения и кольца вычетов.

Определение 1. $\forall n \in \mathbb{N}, n > 1 \; n = p_1^{k_1} \ldots p_s^{k_s}, p_i$ — простые, $p_i \neq p_j$ при $i \neq j$. Оно называется каноническим разложением n.

Теорема 1. (Евклида)

В $\mathbb{N}$ простых чисел бесконечно много.

Доказательство. Пусть $p_1, \ldots p_k$ — все простые числа. $N = p_1 \ldots p_k + 1$. $N \vdots p$, где p — простое. $p = p_i \Rightarrow 1 \vdots p \Rightarrow p \in K^* ?!$

Примеры: $\mathbb{Z}/_{\mathfrak{A}} \; \mathfrak{A} \trianglelefteq \mathbb{Z} \; \mathfrak{A} = <m>, m \in \mathbb{N}_0$.

$<0> \; \mathbb{Z}/_{<0>} = \mathbb{Z}$

$\mathbb{Z}/_{<1>}$ — нулевое кольцо

Определение 2. $\mathbb{Z}/_{<m>}$ называется кольцом вычетов по модулю m.

$\overline{a}$ называют классом вычетов, а a — вычетом.

Определение 3. *Полная система вычетов* по модулю m — это семейство вычетов, обладающее следующими свойствами:

1. Среди членов этого семейства имеются представители всех влассов вычетов по модулю m.
2. Разные члены семейства представляют разные классы.

Замечание 1. Каждую полную систему вычетов можно превратить в кольцо, определив соответствующие операции сложения и умножения.

K — поле. Если $\forall n \in \mathbb{N}\ n1_K \neq 0_K$, то $\operatorname{char} K = 0$.

Если $\exists n \in \mathbb{N} | n1_K = 0$, то $\operatorname{char} K$ — это наименьшее из таких n.

$\operatorname{char}(\mathbb{Z}/_{<p>}) = p$

Предложение 1. K — поле $\Rightarrow \operatorname{char} K = 0 \vee \operatorname{char} K$ — простое число

Доказательство. n — наименьшее число из $\mathbb{N}$, для которого $n1_K = 0_K$. n — непростое: $n = n_1 n_2 \quad n_1, n_2 < n$

$(n_1 1_K)(n_2 1_K) = \underbrace{(1_K + \cdots + 1_K)}_{n_1}\underbrace{(1_K + \cdots + 1_K)}_{n_2} = \underbrace{1_K + \cdots + 1_K}_{n_1 n_2} \Rightarrow n_1 1_K = 0 \vee n_2 1_K = 0_K$?!

Замечание 1. Известные числовые поля ($\mathbb{Q}$, $\mathbb{R}$) — это поля с нулевой характеристикой.

$\mathbb{Z}/_{<m>}$ — коммутативное кольцо с 1.

$\overline{a} \in (\mathbb{Z}/_{<m>})^*$

Предложение 2. $\overline{a} \in (\mathbb{Z}/_{<m>})^* \Leftrightarrow a$ и b взаимно просты.

Доказательство. $\overline{a} \in (\mathbb{Z}/_{<m>})^* \Leftrightarrow \exists \overline{b} \in (\mathbb{Z}/_{<m>})^* | \overline{a}\overline{b} = \overline{1} \Leftrightarrow \exists q \in \mathbb{Z} : ab - 1 = mq, 1 = ab + m(-q) \Leftrightarrow a$ и m взаимно просты.