Министерство образования и науки РФ
Уральский государственный экономический университет

Ю. Б. Мельников

Поле. Расширения полей

Раздел **электронного учебника**
для сопровождения лекции

Изд. 4-е, испр. и доп.

e-mail: melnikov@k66.ru,
melnikov@r66.ru
сайты:
http://melnikov.k66.ru,
http://melnikov.web.ur.ru

Екатеринбург
2012

I. Определение группы

Определение 1. *Универсальная алгебра* $\langle G, \{*, e\}\rangle$ *называется* **группой**, *если двуместная операция* $*$ *и элемент* e *из* G *удовлетворяют следующим трем условиям (аксиомам группы):*

G1. $(x * y) * z = x * (y * z)$ *(ассоциативность);*

G2. *Для любого элемента* g *из* G *справедливо соотношение* $g * e = e * g = g$ *(наличие нейтрального элемента);*

G3. *Для любого элемента* g *из* G *найдется такой элемент* g', *что* $g * g' = e$ *(наличие обратного элемента).*

Элемент g' *называется* **обратным** *к* g.

I. Определение группы

Определение 1. *Универсальная алгебра* $\langle G, \{*, e\}\rangle$ *называется* **группой**, *если двуместная операция* $*$ *и элемент* e *из* G *удовлетворяют следующим трем условиям (аксиомам группы):*

G1. $(x * y) * z = x * (y * z)$ *(ассоциативность);*

G2. *Для любого элемента* g *из* G *справедливо соотношение* $g * e = e * g = g$ *(наличие нейтрального элемента);*

G3. *Для любого элемента* g *из* G *найдется такой элемент* g', *что* $g * g' = e$ *(наличие обратного элемента).*

Элемент g' *называется* **обратным** *к* g.

Определение 2. *Группа* G *называется* **абелевой** *или* **коммутативной**, *если выполняется тождество* $x * y = y * x$ *для любых* $x, y \in G$.

II. Определение поля

Аксиомы группы: **G1)** $(x * y) * z = x * (y * z)$;
G2) $g * e = e * g = g$; **G3)** $g * g' = e$.

Определение 3. Полем *называется такая универсальная алгебра с носителем* P *и сигнатурой* $\{+, *, 0, 1\}$, *что выполняются следующие аксиомы:*

F1. $\langle P, \{+, 0\}\rangle$ — ***абелева группа*** *(**аддитивная** группа поля);*

F2. $\langle P \setminus \{0\}, \{*, 1\}\rangle$ — ***абелева группа*** *(**мультипликативная** группа поля);*

F3. *для любых* x, y, z *из* P *выполняется равенство* $x * (y + z) = x * y +$ *(дистрибутивность).*

II. Определение поля

Аксиомы группы: **G1)** $(x * y) * z = x * (y * z)$;
G2) $g * e = e * g = g$; **G3)** $g * g' = e$.

Поле: **F1)** $\langle P, \{+, 0\}\rangle$ — (абелева) аддитивная группа поля;
F2) $\langle P \setminus \{0\}, \{*, 1\}\rangle$ — (абелева) мультипликативная группа поля;
F3) $x * (y + z) = x * y + x * z$ (дистрибутивность).

Как разобраться с тем, что такое поле?

II. Определение поля

Аксиомы группы: **G1)** $(x * y) * z = x * (y * z)$;
G2) $g * e = e * g = g$; **G3)** $g * g' = e$.

Поле: **F1)** $\langle P, \{+, 0\}\rangle$ — (абелева) аддитивная группа поля;
F2) $\langle P \setminus \{0\}, \{*, 1\}\rangle$ — (абелева) мультипликативная группа поля;
F3) $x * (y + z) = x * y + x * z$ (дистрибутивность).

Есть два стандартных способа: изучение определения (получение следствий) и

II. Определение поля

Аксиомы группы: **G1)** $(x * y) * z = x * (y * z)$;
G2) $g * e = e * g = g$; **G3)** $g * g' = e$.

Поле: **F1)** $\langle P, \{+, 0\}\rangle$ — (абелева) аддитивная группа поля;
F2) $\langle P \backslash \{0\}, \{*, 1\}\rangle$ — (абелева) мультипликативная группа поля;
F3) $x * (y + z) = x * y + x * z$ (дистрибутивность).

Есть два стандартных способа: изучение определения (получение следствий) и
рассмотрение достаточно большого числа примеров.

II.1. Примеры полей

Алгебра $\langle \mathbb{Q}, \{+, \cdot, 0, 1\} \rangle$ является полем и называется **полем рациональных чисел**.

Рациональным числом называется число, представимое в виде $\frac{m}{n}$, где m — целое число, то есть $m \in \mathbb{Z} = \{0; -1; 1; -2; 2; \ldots\}$, и n — натуральное число, то есть $n \in \mathbb{N} = \{1; 2; 3; \ldots\}$. Ниже будет приведена процедура, с помощью которой осуществляется формальное построение поля рациональных чисел, как поля частных кольца целых чисел.

II.1. Примеры полей

Алгебра $\langle \mathbb{Q}, \{+, \cdot, 0, 1\}\rangle$ является полем и называется **полем рациональных чисел**.

Рациональным числом называется число, представимое в виде $\frac{m}{n}$, где m — целое число, то есть $m \in \mathbb{Z} = \{0; -1; 1; -2; 2; \ldots\}$, и n — натуральное число, то есть $n \in \mathbb{N} = \{1; 2; 3; \ldots\}$. Ниже будет приведена процедура, с помощью которой осуществляется формальное построение поля рациональных чисел, как поля частных кольца целых чисел.

Алгебра $\langle \mathbb{R}, \{+, \cdot, 0, 1\}\rangle$ является полем и называется **полем действительных чисел**.

II.1. Примеры полей

Какие еще примеры полей следует рассмотреть в первую очередь?

Показать список базовых исследовательских стратегий?

II.1. Примеры полей

Какие еще примеры полей следует рассмотреть в первую очередь?

Показать список базовых исследовательских стратегий?

Естественно применить стратегию приоритетного изучения «экстремальных» ситуаций. Какие характеристики можно сопоставить полю?

II.1. Примеры полей

Какие еще примеры полей следует рассмотреть в первую очередь?

Показать список базовых исследовательских стратегий?

Естественно применить стратегию приоритетного изучения «экстремальных» ситуаций. Какие характеристики можно сопоставить полю?

В первую очередь, для конечного поля, — *количество элементов*.

II.1. Примеры полей

Какие еще примеры полей следует рассмотреть в первую очередь?

Показать список базовых исследовательских стратегий?

Естественно применить стратегию приоритетного изучения «экстремальных» ситуаций. Какие характеристики можно сопоставить полю?

В первую очередь, для конечного поля, — *количество элементов*.

Ограничено ли сверху число элементов поля, нам пока неизвестно.

II.1. Примеры полей

Какие еще примеры полей следует рассмотреть в первую очередь?

Показать список базовых исследовательских стратегий?

Естественно применить стратегию приоритетного изучения «экстремальных» ситуаций. Какие характеристики можно сопоставить полю?

В первую очередь, для конечного поля, — *количество элементов*.

Поэтому следует посмотреть устройство поля из минимального числа элементов. Каково это число?

Поле: F1) $\langle P, \{+, 0\}\rangle$ — (абелева) аддитивная группа поля;
F2) $\langle P \setminus \{0\}, \{*, 1\}\rangle$ — (абелева) мультипликативная группа поля;
F3) $x * (y + z) = x * y + x * z$ (дистрибутивность).

II.1. Примеры полей

Какие еще примеры полей следует рассмотреть в первую очередь?

Показать список базовых исследовательских стратегий?

Естественно применить стратегию приоритетного изучения «экстремальных» ситуаций. Какие характеристики можно сопоставить полю?

В первую очередь, для конечного поля, — *количество элементов*.

Ясно, что в поле не меньше двух элементов, так как в мультипликативной группе есть хотя бы один элемент (единичный).

Поле: F1) $\langle P, \{+, 0\}\rangle$ — (абелева) аддитивная группа поля;
F2) $\langle P \setminus \{0\}, \{*, 1\}\rangle$ — (абелева) мультипликативная группа поля;
F3) $x * (y + z) = x * y + x * z$ (дистрибутивность).

II.1. Примеры полей

Построим поле из двух элементов. Обозначим через 0 нулевой элемент поля, и через 1 — единичный элемент, т.е. единичный элемент мультипликативной группы поля.

II.1. Примеры полей

Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0+0=0$, $0+1=1=1+0$. Чему равно $1+1$?

II.1. Примеры полей

Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0+0=0$, $0+1=1=1+0$. Чему равно $1+1$?

Так как относительно сложения поле есть группа, то у 1 должен быть обратный элемент. $1+(-1)=0$. Ура?

II.1. Примеры полей

Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0+0=0$, $0+1=1=1+0$. Чему равно $1+1$?

Так как относительно сложения поле есть группа, то у 1 должен быть обратный элемент. $1+(-1)=0$. Но (-1) — это элемент поля, т.е. это либо 0, либо 1. Ясно, что это не 0, так как $1+0=$

II.1. Примеры полей

Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0+0=0$, $0+1=1=1+0$. Чему равно $1+1$?

Так как относительно сложения поле есть группа, то у 1 должен быть обратный элемент. $1+(-1)=0$. Но (-1) — это элемент поля, т.е. это либо 0, либо 1. Ясно, что это не 0, так как $1+0=1\neq 0$.

II.1. Примеры полей

Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0+0=0$, $0+1=1=1+0$. Чему равно $1+1$?

Так как относительно сложения поле есть группа, то у 1 должен быть обратный элемент. $1+(-1)=0$. Но (-1) — это элемент поля, т.е. это либо 0, либо 1. Значит, $(-1)=1$.

II.1. Примеры полей

Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0+0=0$, $0+1=1=1+0$. Получили, что $1+1=0$.

Как-то не так было в первом классе :)

II.1. Примеры полей

Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0 + 0 = 0$, $0 + 1 = 1 = 1 + 0$. Получили, что $1 + 1 = 0$.

Разберемся с умножением. Ясно, что $1 * 1 = 1$, так как

II.1. Примеры полей

Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0+0=0$, $0+1=1=1+0$. Получили, что $1+1=0$.

Разберемся с умножением. Ясно, что $1*1=1$, так как 1 — нейтральный элемент e группы.

Аксиомы группы: G1) $(x*y)*z=x*(y*z)$;
G2) $g*e=e*g=g$; G3) $g*g'=e$.

II.1. Примеры полей

Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0 + 0 = 0$, $0 + 1 = 1 = 1 + 0$. Получили, что $1 + 1 = 0$.

Разберемся с умножением. Имеем $1 * 1 = 1$. Чему равно $1 * 0$?

II.1. Примеры полей

Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0+0=0$, $0+1=1=1+0$. Получили, что $1+1=0$.

Разберемся с умножением. Имеем $1*1=1$. Чему равно $1*0$? Свойство 0 как нейтрального элемента группы, с умножением связывает только одно свойство.

Поле: F1) $\langle P, \{+,0\}\rangle$ — (абелева) аддитивная группа поля;
F2) $\langle P\setminus\{0\}, \{*,1\}\rangle$ — (абелева) мультипликативная группа поля;
F3) $x*(y+z)=x*y+x*z$ (дистрибутивность).

II.1. Примеры полей

Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0+0=0$, $0+1=1=1+0$. Получили, что $1+1=0$.

Разберемся с умножением. Имеем $1*1=1$. Чему равно $1*0$? Свойство 0 как нейтрального элемента группы, с умножением связывает только одно свойство F3.

Поле: F1) $\langle P, \{+,0\}\rangle$ — (абелева) аддитивная группа поля;
F2) $\langle P\setminus\{0\}, \{*,1\}\rangle$ — (абелева) мультипликативная группа поля;
F3) $x*(y+z)=x*y+x*z$ (дистрибутивность).

II.1. Примеры полей

Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0+0=0$, $0+1=1=1+0$. Получили, что $1+1=0$.

Разберемся с умножением. Имеем $1*1=1$. Чему равно $1*0$? Свойство 0 как нейтрального элемента группы, с умножением связывает только одно свойство F3.

Поле: F1) $\langle P, \{+,0\}\rangle$ — (абелева) аддитивная группа поля;
F2) $\langle P\setminus\{0\}, \{*,1\}\rangle$ — (абелева) мультипликативная группа поля;
F3) $x*(y+z)=x*y+x*z$ (дистрибутивность).

$$1*(1+0)=1*1+1*0$$

II.1. Примеры полей

Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0+0=0$, $0+1=1=1+0$. Получили, что $1+1=0$.

Разберемся с умножением. Имеем $1*1=1$. Чему равно $1*0$? Свойство 0 как нейтрального элемента группы, с умножением связывает только одно свойство F3.

Поле: F1) $\langle P, \{+,0\}\rangle$ — (абелева) аддитивная группа поля;
F2) $\langle P\setminus\{0\}, \{*,1\}\rangle$ — (абелева) мультипликативная группа поля;
F3) $x*(y+z)=x*y+x*z$ (дистрибутивность).

$$1*1=1*(1+0)=1*1+1*0$$

II.1. Примеры полей

Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0+0=0$, $0+1=1=1+0$. Получили, что $1+1=0$.

Разберемся с умножением. Имеем $1*1=1$. Чему равно $1*0$? Свойство 0 как нейтрального элемента группы, с умножением связывает только одно свойство F3.

Поле: F1) $\langle P, \{+,0\}\rangle$ — (абелева) аддитивная группа поля; F2) $\langle P\setminus\{0\}, \{*,1\}\rangle$ — (абелева) мультипликативная группа поля; F3) $x*(y+z)=x*y+x*z$ (дистрибутивность).

$1=1*1=1*(1+0)=1*1+1*0$.

II.1. Примеры полей

Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0+0=0$, $0+1=1=1+0$. Получили, что $1+1=0$.

Разберемся с умножением. Имеем $1*1=1$. Чему равно $1*0$? Свойство 0 как нейтрального элемента группы, с умножением связывает только одно свойство F3.

Поле: F1) $\langle P, \{+,0\}\rangle$ — (абелева) аддитивная группа поля;
F2) $\langle P\setminus\{0\}, \{*,1\}\rangle$ — (абелева) мультипликативная группа поля;
F3) $x*(y+z)=x*y+x*z$ (дистрибутивность).

$1=1*1=1*(1+0)=1*1+1*0=1+1*0$. Значит, $1=1+1*0$.

II.1. Примеры полей

Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0+0=0$, $0+1=1=1+0$. Получили, что $1+1=0$.

Разберемся с умножением. Имеем $1*1=1$. Чему равно $1*0$? Свойство 0 как нейтрального элемента группы, с умножением связывает только одно свойство F3.

Поле: F1) $\langle P, \{+,0\}\rangle$ — (абелева) аддитивная группа поля;
F2) $\langle P\setminus\{0\}, \{*,1\}\rangle$ — (абелева) мультипликативная группа поля;
F3) $x*(y+z)=x*y+x*z$ (дистрибутивность).

$1=1*1=1*(1+0)=1*1+1*0=1+1*0$. Значит, $1=1+1*0$.

По критерию нейтрального элемента $1*0=0$.

II.1. Примеры полей

Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0+0=0$, $0+1=1=1+0$. Получили, что $1+1=0$.

Разберемся с умножением. Имеем $1*1=1$, $1*0=0=0*1$. Чему равно $0*0$?

II.1. Примеры полей

Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0+0=0$, $0+1=1=1+0$. Получили, что $1+1=0$.

Разберемся с умножением. Имеем $1*1=1$, $1*0=0=0*1$. Чему равно $0*0$?

$0*0=0*(1+1)=0*1+0*1=0+0=0$.

II.1. Примеры полей

Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0+0=0$, $0+1=1=1+0$. Получили, что $1+1=0$.

Разберемся с умножением. Имеем $1*1=1$, $1*0=0=0*1$. Чему равно $0*0$?

$0*0=0*(1+1)=0*1+0*1=0+0=0$. Значит, $0*0=0$.

II.1. Примеры полей

Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0+0=0$, $0+1=1=1+0$. Получили, что $1+1=0$.

Разберемся с умножением. Имеем $1*1=1$, $1*0=0=0*1$, $0*0=0$.

Ура? :) :(

II.1. Примеры полей

Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0+0=0$, $0+1=1=1+0$. Получили, что $1+1=0$.

Разберемся с умножением. Имеем $1*1=1$, $1*0=0=0*1$, $0*0=0$.

Ура?

Надо операции задать стандартным образом!

II.1. Примеры полей

Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0+0=0$, $0+1=1=1+0$. Получили, что $1+1=0$.

Разберемся с умножением. Имеем $1*1=1$, $1*0=0=0*1$, $0*0=0$.

Ура?

Надо операции задать стандартным образом!

Операция — это функция. Стандартными являются следующие способы ее задания:

II.1. Примеры полей

Построим поле из двух элементов.

Сложение с 0 не меняет элементов, поэтому $0+0=0$, $0+1=1=1+0$. Получили, что $1+1=0$.

Разберемся с умножением. Имеем $1*1=1$, $1*0=0=0*1$, $0*0=0$.

Ура?

Надо операции задать стандартным образом!

Операция — это функция. Стандартными являются следующие способы ее задания:
формулой, графиком, таблицей.

Какой способ оптимален для нашего случая?

II.1. Примеры полей

Полем является алгебра $GF(2) = \langle \{0; 1\},\ \{+, \cdot, 0, 1\} \rangle$, где бинарные операции $+, \cdot$ заданы следующими таблицами Кэли:

$x + y$		
$y \backslash x$	0	1
0	0	1
1	1	0

,

$x \cdot y$		
$y \backslash x$	0	1
0	0	0
1	0	1

.

Это поле имеет наименьшее число элементов в носителе.

II.2. Теорема об умножении на нуль в поле

Перейдем к другому способу изучения поля — получению следствий из аксиом (дедуктивный способ). Одну теорему мы уже доказали, когда строили поле $GF(2)$.

II.2. Теорема об умножении на нуль в поле

Теорема 1 (**об умножении на нуль в поле**). *Для любого x из P имеет место равенство $x * 0 = 0$.*

Доказательство.

II.2. Теорема об умножении на нуль в поле

Теорема 1 (**об умножении на нуль в поле**). *Для любого x из P имеет место равенство $x * 0 = 0$.*

Доказательство. $x + x * 0 =$

II.2. Теорема об умножении на нуль в поле

Теорема 1 (**об умножении на нуль в поле**). *Для любого x из P имеет место равенство $x * 0 = 0$.*

Доказательство. $x + x * 0 = x * 1 + x * 0 =$

II.2. Теорема об умножении на нуль в поле

Теорема 1 (**об умножении на нуль в поле**). *Для любого x из P имеет место равенство $x * 0 = 0$.*

Доказательство. $x + x * 0 = x * 1 + x * 0 = x * (1 + 0) =$

II.2. Теорема об умножении на нуль в поле

Теорема 1 (**об умножении на нуль в поле**). *Для любого x из P имеет место равенство $x * 0 = 0$.*

Доказательство. $x + x * 0 = x * 1 + x * 0 = x * (1 + 0) = x * 1 =$

II.2. Теорема об умножении на нуль в поле

Теорема 1 (**об умножении на нуль в поле**). *Для любого x из P имеет место равенство $x * 0 = 0$.*

Доказательство. $x + x * 0 = x * 1 + x * 0 = x * (1 + 0) = x * 1 = x$.

II.2. Теорема об умножении на нуль в поле

Теорема 1 (**об умножении на нуль в поле**). *Для любого x из P имеет место равенство $x * 0 = 0$.*

Доказательство. $x + x * 0 = x * 1 + x * 0 = x * (1 + 0) = x * 1 = x$.

По критерию нейтрального элемента, примененному к аддитивной группе поля, получаем заключение теоремы: $x * 0 = 0$.

Можно иначе:

II.2. Теорема об умножении на нуль в поле

Теорема 1 (**об умножении на нуль в поле**). *Для любого x из P имеет место равенство $x * 0 = 0$.*

Доказательство. $x + x * 0 = x * 1 + x * 0 = x * (1 + 0) = x * 1 = x$.
Можно иначе: $x + x * 0 = x \ \Rightarrow$

II.2. Теорема об умножении на нуль в поле

Теорема 1 (**об умножении на нуль в поле**). *Для любого x из P имеет место равенство $x * 0 = 0$.*

Доказательство. $x + x * 0 = x * 1 + x * 0 = x * (1 + 0) = x * 1 = x$.
Можно иначе: $x + x * 0 = x \ \Rightarrow \ (-x) + x + x * 0 = (-x) + x$

II.2. Теорема об умножении на нуль в поле

Теорема 1 (**об умножении на нуль в поле**). *Для любого x из P имеет место равенство $x * 0 = 0$.*

Доказательство. $x + x * 0 = x * 1 + x * 0 = x * (1 + 0) = x * 1 = x$.
Можно иначе: $x + x * 0 = x \Rightarrow \underbrace{(-x) + x}_{0} + x * 0 = \underbrace{(-x) + x}_{0}$

II.2. Теорема об умножении на нуль в поле

Теорема 1 (**об умножении на нуль в поле**). *Для любого x из P имеет место равенство $x * 0 = 0$.*

Доказательство. $x + x * 0 = x * 1 + x * 0 = x * (1 + 0) = x * 1 = x$.

Можно иначе: $x + x * 0 = x \ \Rightarrow \ \underbrace{(-x) + x}_{0} + x * 0 = \underbrace{(-x) + x}_{0} \ \Rightarrow$

$\Rightarrow \ 0 + x * 0 = 0 \ \Rightarrow$

II.2. Теорема об умножении на нуль в поле

Теорема 1 (**об умножении на нуль в поле**). *Для любого x из P имеет место равенство $x * 0 = 0$.*

Доказательство. $x + x * 0 = x * 1 + x * 0 = x * (1 + 0) = x * 1 = x$.
Можно иначе: $x + x * 0 = x \;\Rightarrow\; \underbrace{(-x) + x}_{0} + x * 0 = \underbrace{(-x) + x}_{0} \;\Rightarrow$
$\Rightarrow\; 0 + x * 0 = 0 \;\Rightarrow\; x * 0 = 0,$ теорема доказана.

II.3. Теорема о делителях нуля в поле

Теорема 2 (**о делителях нуля в поле**). *Для любых элементов* $x, y \in P$ *имеем* $x * y = \mathbf{0}$ *тогда и только тогда, когда* $x = \mathbf{0}$ *или* $y = \mathbf{0}$.

Доказательство.

Поле: F1) $\langle P, \{+, 0\}\rangle$ — (абелева) аддитивная группа поля;
F2) $\langle P \setminus \{0\}, \{*, 1\}\rangle$ — (абелева) мультипликативная группа поля;
F3) $x * (y + z) = x * y + x * z$ (дистрибутивность).

II.3. Теорема о делителях нуля в поле

Теорема 2 (**о делителях нуля в поле**). *Для любых элементов* $x, y \in P$ *имеем* $x * y = \mathbf{0}$ *тогда и только тогда, когда* $x = \mathbf{0}$ *или* $y = \mathbf{0}$.

Доказательство необходимости. От противного. Если бы $x \neq \mathbf{0} \neq y$, то элемент $x * y$ принадлежал бы мультипликативной группе поля, носитель которой не содержит нуля поля, противоречие.

Поле: F1) $\langle P, \{+, 0\}\rangle$ — (абелева) аддитивная группа поля;
F2) $\langle P \setminus \{0\}, \{*, 1\}\rangle$ — (абелева) мультипликативная группа поля;
F3) $x * (y + z) = x * y + x * z$ (дистрибутивность).

II.3. Теорема о делителях нуля в поле

Теорема 2 (**о делителях нуля в поле**). *Для любых элементов* $x, y \in P$ *имеем* $x * y = \mathbf{0}$ *тогда и только тогда, когда* $x = \mathbf{0}$ *или* $y = \mathbf{0}$.

Достаточность следует из **теоремы об умножении на нуль в поле**.

Поле: F1) $\langle P, \{+, 0\}\rangle$ — (абелева) аддитивная группа поля;
F2) $\langle P \setminus \{0\}, \{*, 1\}\rangle$ — (абелева) мультипликативная группа поля;
F3) $x * (y + z) = x * y + x * z$ (дистрибутивность).

II.4. Характеристика поля

Какие ситуации в поле являются «экстремальными» и, значит, наиболее интересными?

II.4. Характеристика поля

Какие ситуации в поле являются «экстремальными» и, значит, наиболее интересными? Применим стратегию поиска аналогии. Наиболее изученными нами являются поле рациональных и поле действительных чисел. Начиналось все с натуральных чисел. Операция умножения вводилась как кратное сложение:

$$\underbrace{n + n + \ldots + n}_{m \text{ слагаемых}} = m \cdot n.$$

II.4. Характеристика поля

Какие ситуации в поле являются «экстремальными» и, значит, наиболее интересными? Применим стратегию поиска аналогии. Наиболее изученными нами являются поле рациональных и поле действительных чисел. Начиналось все с натуральных чисел. Операция умножения вводилась как кратное сложение:

$$\underbrace{n + n + \ldots + n}_{m \text{ слагаемых}} = m \cdot n.$$

Если n — натуральное число и x — элемент поля, то через nx будем обозначать сумму n штук элементов x из P:

$$nx = \underbrace{x + x + \ldots + x}_{n \text{ штук}}.$$

II.4. Характеристика поля

Какие ситуации в поле являются «экстремальными» и, значит, наиболее интересными? Применим стратегию поиска аналогии. Наиболее изученными нами являются поле рациональных и поле действительных чисел. Начиналось все с натуральных чисел. Операция умножения вводилась как кратное сложение:

$$\underbrace{n + n + \ldots + n}_{m \text{ слагаемых}} = m \cdot n.$$

Если n — натуральное число и x — элемент поля, то через nx будем обозначать сумму n штук элементов x из P:

$$nx = \underbrace{x + x + \ldots + x}_{n \text{ штук}}.$$

Внимание!!! nx — **это не умножение! Это кратное сложение!**

II.4. Характеристика поля

Какие ситуации в поле являются «экстремальными» и, значит, наиболее интересными?

Если n — натуральное число и x — элемент поля, то через nx будем обозначать сумму n штук элементов x из P:

$$nx = \underbrace{x + x + \ldots + x}_{n \text{ штук}}.$$

Внимание!!! nx — **это не умножение! Это кратное сложение!**

Если поле конечное, то среди элементов x, $2x$, $3x$,... есть одинаковые.

Ну, и что? :(

II.4. Характеристика поля

Какие ситуации в поле являются «экстремальными» и, значит, наиболее интересными?

Если n — натуральное число и x — элемент поля, то через nx будем обозначать сумму n штук элементов x из P:

$$nx = \underbrace{x + x + \ldots + x}_{n \text{ штук}}.$$

Внимание!!! nx — **это не умножение! Это кратное сложение!**

Если поле конечное, то среди элементов x, $2x$, $3x$,... есть одинаковые.

Значит, для некоторых натуральных $n > m$ имеем $nx = mx$.

II.4. Характеристика поля

Какие ситуации в поле являются «экстремальными» и, значит, наиболее интересными?

Если n — натуральное число и x — элемент поля, то через nx будем обозначать сумму n штук элементов x из P:

$$nx = \underbrace{x + x + \ldots + x}_{n \text{ штук}}.$$

Внимание!!! nx — **это не умножение! Это кратное сложение!**

Если поле конечное, то среди элементов x, $2x$, $3x$,... есть одинаковые.

Значит, для некоторых натуральных $n > m$ имеем $nx = mx$. Умножим обе части равенства на x^{-1} (**мультипликативный** обратный к x).

II.4. Характеристика поля

Какие ситуации в поле являются «экстремальными» и, значит, наиболее интересными?

Если n — натуральное число и x — элемент поля, то через nx будем обозначать сумму n штук элементов x из P:

$$nx = \underbrace{x + x + \ldots + x}_{n \text{ штук}}.$$

Внимание!!! nx — **это не умножение! Это кратное сложение!**

Если поле конечное, то среди элементов x, $2x$, $3x$,... есть одинаковые.

Значит, для некоторых натуральных $n > m$ имеем $nx = mx$. Умножим обе части равенства на x^{-1}. Получим $n1 = m1$.

II.4. Характеристика поля

Какие ситуации в поле являются «экстремальными» и, значит, наиболее интересными?

Если n — натуральное число и x — элемент поля, то через nx будем обозначать сумму n штук элементов x из P:

$$nx = \underbrace{x + x + \ldots + x}_{n \text{ штук}}.$$

Внимание!!! nx — **это не умножение! Это кратное сложение!**

Если поле конечное, то среди элементов x, $2x$, $3x$,... есть одинаковые.

Значит, для некоторых натуральных $n > m$ имеем $nx = mx$. Умножим обе части равенства на x^{-1}. Получим $n1 = m1$, откуда вычитая $m1$ из обеих частей равенства, получаем $(n - m)1 = 0$.

II.4. Характеристика поля

Какие ситуации в поле являются «экстремальными» и, значит, наиболее интересными?

Если n — натуральное число и x — элемент поля, то через nx будем обозначать сумму n штук элементов x из P:

$$nx = \underbrace{x + x + \ldots + x}_{n \text{ штук}}.$$

Внимание!!! nx — **это не умножение! Это кратное сложение!**

Если поле конечное, то среди элементов x, $2x$, $3x$,... есть одинаковые.

Значит, для некоторых натуральных $n > m$ имеем $nx = mx$. Умножим обе части равенства на x^{-1}. Получим $n1 = m1$, откуда вычитая $m1$ из обеих частей равенства, получаем $(n - m)1 = 0$.

Наиболее интересен «экстремальный» случай, когда $(n - m)$ — минимальное с этим свойством.

II.4. Характеристика поля

Определение 4. *Если существует такое натуральное число* n, *что* $n1 = \underbrace{1+1+\ldots+1}_{n \text{ слагаемых}} = 0$, *то наименьшее такое число* n *называется* **характеристикой поля** P. *Если такое* n *не существует, то есть для любого натурального числа* n *имеем* $n1 \neq 0$, *то* **характеристику поля** *считают равной 0. Характеристика поля* P *обозначается через* $\mathrm{char}(P)$.

Внимание!!! nx — это не умножение! Это кратное сложение!

II.5. Критерий характеристики поля

Теорема 3. *Ненулевое число n является* ***характеристикой поля*** *тогда и только тогда, когда*

$$\forall x \in F \quad \left(x \neq 0 \;\Rightarrow\; nx = \underbrace{x + x + \ldots + x + x}_{n \text{ слагаемых}} = 0 \right), \qquad (1)$$

причем $\forall m \quad 1 \leq m < n \;\Rightarrow\; mx \neq 0$.

Доказательство.

II.5. Критерий характеристики поля

Теорема 3. *Ненулевое число n является* ***характеристикой поля*** *тогда и только тогда, когда*

$$\forall x \in F \quad \left(x \neq 0 \;\Rightarrow\; nx = \underbrace{x + x + \ldots + x + x}_{n \text{ слагаемых}} = 0 \right), \qquad (1)$$

причем $\forall m \quad 1 \leq m < n \;\Rightarrow\; mx \neq 0.$

Доказательство. Пусть $x \neq 0$ и n — **характеристика поля** F.

$$n1 =$$

II.5. Критерий характеристики поля

Теорема 3. *Ненулевое число n является* ***характеристикой поля*** *тогда и только тогда, когда*

$$\forall x \in F \quad \left(x \neq 0 \;\Rightarrow\; nx = \underbrace{x + x + \ldots + x + x}_{n \text{ слагаемых}} = 0 \right), \qquad (1)$$

причем $\forall m \quad 1 \leq m < n \;\Rightarrow\; mx \neq 0.$

Доказательство. Пусть $x \neq 0$ и n — **характеристика поля** F.

$$n1 = \underbrace{1 + 1 + \ldots + 1}_{n \text{ слагаемых}} =$$

II.5. Критерий характеристики поля

Теорема 3. *Ненулевое число n является* ***характеристикой поля*** *тогда и только тогда, когда*

$$\forall x \in F \quad \left(x \neq 0 \;\Rightarrow\; nx = \underbrace{x + x + \ldots + x + x}_{n \text{ слагаемых}} = 0 \right), \qquad (1)$$

причем $\forall m \quad 1 \leq m < n \;\Rightarrow\; mx \neq 0.$

Доказательство. Пусть $x \neq 0$ и n — **характеристика поля** F.

$$n1 = \underbrace{1 + 1 + \ldots + 1}_{n \text{ слагаемых}} = 0 \;\Rightarrow$$

II.5. Критерий характеристики поля

Теорема 3. *Ненулевое число n является* ***характеристикой поля*** *тогда и только тогда, когда*

$$\forall x \in F \quad \left(x \neq 0 \;\Rightarrow\; nx = \underbrace{x + x + \ldots + x + x}_{n \text{ слагаемых}} = 0 \right), \qquad (1)$$

причем $\forall m \quad 1 \leq m < n \;\Rightarrow\; mx \neq 0.$

Доказательство. Пусть $x \neq 0$ и n — **характеристика поля** F.

$$n1 = \underbrace{1 + 1 + \ldots + 1}_{n \text{ слагаемых}} = 0 \;\Rightarrow\; \underbrace{(1 + 1 + \ldots + 1)}_{n \text{ слагаемых}} \cdot x = 0 \cdot x \;\Rightarrow$$

II.5. Критерий характеристики поля

Теорема 3. *Ненулевое число n является* ***характеристикой поля*** *тогда и только тогда, когда*

$$\forall x \in F \quad \left(x \neq 0 \;\Rightarrow\; nx = \underbrace{x + x + \ldots + x + x}_{n \text{ слагаемых}} = 0 \right), \qquad (1)$$

причем $\forall m \quad 1 \leq m < n \;\Rightarrow\; mx \neq 0.$

Доказательство. Пусть $x \neq 0$ и n — **характеристика поля** F.

$$n1 = \underbrace{1 + 1 + \ldots + 1}_{n \text{ слагаемых}} = 0 \;\Rightarrow\; \underbrace{(1 + 1 + \ldots + 1)}_{n \text{ слагаемых}} \cdot x = 0 \cdot x \;\Rightarrow$$

$$\Rightarrow\; \underbrace{(x + x + \ldots + x)}_{n \text{ слагаемых}} = 0.$$

II.5. Критерий характеристики поля

Теорема 3. *Ненулевое число n является* ***характеристикой поля*** *тогда и только тогда, когда*

$$\forall x \in F \quad \left(x \neq 0 \;\Rightarrow\; nx = \underbrace{x + x + \ldots + x + x}_{n \text{ слагаемых}} = 0 \right), \qquad (1)$$

причем $\forall m \quad 1 \leq m < n \;\Rightarrow\; mx \neq 0.$

Доказательство. Пусть $x \neq 0$ и n — **характеристика поля** F.

$$n1 = \underbrace{1 + 1 + \ldots + 1}_{n \text{ слагаемых}} = 0 \;\Rightarrow\; \underbrace{(1 + 1 + \ldots + 1)}_{n \text{ слагаемых}} \cdot x = 0 \cdot x \;\Rightarrow$$

$$\Rightarrow\; \underbrace{(x + x + \ldots + x)}_{n \text{ слагаемых}} = 0.$$

Значит, $nx = \underbrace{(x + x + \ldots + x)}_{n \text{ слагаемых}} = 0.$

II.5. Критерий характеристики поля

Теорема 3. *Ненулевое число n является* ***характеристикой поля*** *тогда и только тогда, когда*

$$\forall x \in F \quad \left(x \neq 0 \;\Rightarrow\; nx = \underbrace{x + x + \ldots + x + x}_{n \text{ слагаемых}} = 0 \right), \qquad (1)$$

причем $\forall m \quad 1 \leq m < n \;\Rightarrow\; mx \neq 0$.

Доказательство. Пусть $x \neq 0$ и n — **характеристика поля** F. Тогда $nx = 0$. Пусть m — минимальное такое натуральное число, для которого в F существует ненулевой элемент x со свойством $mx = 0$.

II.5. Критерий характеристики поля

Теорема 3. *Ненулевое число n является* ***характеристикой поля*** *тогда и только тогда, когда*

$$\forall x \in F \quad \left(x \neq 0 \;\Rightarrow\; nx = \underbrace{x + x + \ldots + x + x}_{n \text{ слагаемых}} = 0 \right), \qquad (1)$$

причем $\forall m \quad 1 \leq m < n \;\Rightarrow\; mx \neq 0.$

Доказательство. Пусть $x \neq 0$ и n — **характеристика поля** F. Тогда $nx = 0$. Пусть m — минимальное такое натуральное число, для которого в F существует ненулевой элемент x со свойством $mx = 0$.

$$\underbrace{(x + x + \ldots + x)}_{m \text{ слагаемых}} = 0 \;\Rightarrow$$

II.5. Критерий характеристики поля

Теорема 3. *Ненулевое число n является* ***характеристикой поля*** *тогда и только тогда, когда*

$$\forall x \in F \quad \left(x \neq 0 \;\Rightarrow\; nx = \underbrace{x + x + \ldots + x + x}_{n \text{ слагаемых}} = 0 \right), \qquad (1)$$

причем $\forall m \quad 1 \leq m < n \;\Rightarrow\; mx \neq 0.$

Доказательство. Пусть $x \neq 0$ и n — **характеристика поля** F. Тогда $nx = 0$. Пусть m — минимальное такое натуральное число, для которого в F существует ненулевой элемент x со свойством $mx = 0$.

$$\underbrace{(x + x + \ldots + x)}_{m \text{ слагаемых}} = 0 \;\Rightarrow\; \underbrace{(1 + 1 + \ldots + 1)}_{m \text{ слагаемых}} \cdot x = 0 \;\Rightarrow$$

II.5. Критерий характеристики поля

Теорема 3. *Ненулевое число n является* ***характеристикой поля*** *тогда и только тогда, когда*

$$\forall x \in F \quad \left(x \neq 0 \;\Rightarrow\; nx = \underbrace{x + x + \ldots + x + x}_{n \text{ слагаемых}} = 0 \right), \qquad (1)$$

причем $\forall m \quad 1 \leq m < n \;\Rightarrow\; mx \neq 0.$

Доказательство. Пусть $x \neq 0$ и n — **характеристика поля** F. Тогда $nx = 0$. Пусть m — минимальное такое натуральное число, для которого в F существует ненулевой элемент x со свойством $mx = 0$.

$$\underbrace{(x + x + \ldots + x)}_{m \text{ слагаемых}} = 0 \;\Rightarrow\; \underbrace{(1 + 1 + \ldots + 1)}_{m \text{ слагаемых}} \cdot x = 0 \;\Rightarrow$$

$$\Rightarrow\; \underbrace{(1 + 1 + \ldots + 1)}_{m \text{ слагаемых}} \cdot x \cdot x^{-1} = 0 \cdot x^{-1} \;\Rightarrow$$

II.5. Критерий характеристики поля

Теорема 3. *Ненулевое число n является* ***характеристикой поля*** *тогда и только тогда, когда*

$$\forall x \in F \quad \left(x \neq 0 \;\Rightarrow\; nx = \underbrace{x + x + \ldots + x + x}_{n \text{ слагаемых}} = 0 \right), \qquad (1)$$

причем $\forall m \quad 1 \leq m < n \;\Rightarrow\; mx \neq 0.$

Доказательство. Пусть $x \neq 0$ и n — **характеристика поля** F. Тогда $nx = 0$. Пусть m — минимальное такое натуральное число, для которого в F существует ненулевой элемент x со свойством $mx = 0$.

$$\underbrace{(x + x + \ldots + x)}_{m \text{ слагаемых}} = 0 \;\Rightarrow\; \underbrace{(1 + 1 + \ldots + 1)}_{m \text{ слагаемых}} \cdot x = 0 \;\Rightarrow$$

$$\Rightarrow\; \underbrace{(1 + 1 + \ldots + 1)}_{m \text{ слагаемых}} \cdot x \cdot x^{-1} = 0 \cdot x^{-1} \;\Rightarrow\; \underbrace{1 + 1 + \ldots + 1}_{m \text{ слагаемых}} = 0.$$

II.5. Критерий характеристики поля

Теорема 3. *Ненулевое число n является* ***характеристикой поля*** *тогда и только тогда, когда*

$$\forall x \in F \quad \left(x \neq 0 \;\Rightarrow\; nx = \underbrace{x + x + \ldots + x + x}_{n \text{ слагаемых}} = 0 \right), \qquad (1)$$

причем $\forall m \quad 1 \leq m < n \;\Rightarrow\; mx \neq 0.$

Доказательство. Пусть $x \neq 0$ и n — **характеристика поля** F. Тогда $nx = 0$. Пусть m — минимальное такое натуральное число, для которого в F существует ненулевой элемент x со свойством $mx = 0$.

$$\underbrace{(x + x + \ldots + x)}_{m \text{ слагаемых}} = 0 \;\Rightarrow\; \underbrace{1 + 1 + \ldots + 1}_{m \text{ слагаемых}} = 0.$$

Следовательно, $n \leq m \leq$

II.5. Критерий характеристики поля

Теорема 3. *Ненулевое число n является* ***характеристикой поля*** *тогда и только тогда, когда*

$$\forall x \in F \quad \left(x \neq 0 \;\Rightarrow\; nx = \underbrace{x + x + \ldots + x + x}_{n \text{ слагаемых}} = 0 \right), \qquad (1)$$

причем $\forall m \quad 1 \leq m < n \;\Rightarrow\; mx \neq 0.$

Доказательство. Пусть $x \neq 0$ и n — **характеристика поля** F. **Тогда** $nx = 0.$ Пусть m — минимальное такое натуральное число, для которого в F существует ненулевой элемент x со свойством $mx = 0$.

$$\underbrace{(x + x + \ldots + x)}_{m \text{ слагаемых}} = 0 \;\Rightarrow\; \underbrace{1 + 1 + \ldots + 1}_{m \text{ слагаемых}} = 0.$$

Следовательно, $n \leq m \leq$

II.5. Критерий характеристики поля

Теорема 3. *Ненулевое число n является* ***характеристикой поля*** *тогда и только тогда, когда*

$$\forall x \in F \quad \left(x \neq 0 \;\Rightarrow\; nx = \underbrace{x + x + \ldots + x + x}_{n \text{ слагаемых}} = 0 \right), \qquad (1)$$

причем $\forall m \quad 1 \leq m < n \;\Rightarrow\; mx \neq 0.$

Доказательство. Пусть $x \neq 0$ и n — **характеристика поля** F. **Тогда** $nx = 0$. Пусть m — минимальное такое натуральное число, для которого в F существует ненулевой элемент x со свойством $mx = 0$.

$$\underbrace{(x + x + \ldots + x)}_{m \text{ слагаемых}} = 0 \;\Rightarrow\; \underbrace{1 + 1 + \ldots + 1}_{m \text{ слагаемых}} = 0.$$

Следовательно, $n \leq m \leq n$.

II.5. Критерий характеристики поля

Теорема 3. *Ненулевое число n является* ***характеристикой поля*** *тогда и только тогда, когда*

$$\forall x \in F \quad \left(x \neq 0 \;\Rightarrow\; nx = \underbrace{x + x + \ldots + x + x}_{n \text{ слагаемых}} = 0 \right), \qquad (1)$$

причем $\forall m \quad 1 \leq m < n \;\Rightarrow\; mx \neq 0.$

Доказательство. Пусть $x \neq 0$ и n — **характеристика поля** F. Тогда $nx = 0$. Пусть m — минимальное такое натуральное число, для которого в F существует ненулевой элемент x со свойством $mx = 0$.

$$\underbrace{(x + x + \ldots + x)}_{m \text{ слагаемых}} = 0 \;\Rightarrow\; \underbrace{1 + 1 + \ldots + 1}_{m \text{ слагаемых}} = 0.$$

Следовательно, $n \leq m \leq n$. Теорема доказана.

II.6. Теорема о простоте ненулевой характеристики поля

Теорема 4 (**о простоте ненулевой характеристики поля**). *Характеристика поля является либо нулем, либо простым числом.*

Доказательство.

II.6. Теорема о простоте ненулевой характеристики поля

Теорема 4 (о простоте ненулевой характеристики поля). *Характеристика поля является либо нулем, либо простым числом.*

Доказательство. Пусть n — ненулевая характеристика поля P и $n = p \cdot q$, где p — простое число. Докажем, что для любого x из P имеет место $px = 0$.

II.6. Теорема о простоте ненулевой характеристики поля

Теорема 4 (о простоте ненулевой характеристики поля). *Характеристика поля является либо нулем, либо простым числом.*

Доказательство. Пусть n — ненулевая характеристика поля P и $n = p \cdot q$, где p — простое число. Докажем, что для любого x из P имеет место $px = 0$.

Пусть в $P \setminus \{0\}$ имеется такой элемент z, что $pz = 0$.

II.6. Теорема о простоте ненулевой характеристики поля

Теорема 4 (**о простоте ненулевой характеристики поля**). *Характеристика поля является либо нулем, либо простым числом.*

Доказательство. Пусть n — ненулевая характеристика поля P и $n = p \cdot q$, где p — простое число. Докажем, что для любого x из P имеет место $px = 0$.

Пусть в $P \setminus \{0\}$ имеется такой элемент z, что $pz = 0$.

Умножим обе части последнего равенства на z^{-1}. Получим

II.6. Теорема о простоте ненулевой характеристики поля

Теорема 4 (**о простоте ненулевой характеристики поля**). *Характеристика поля является либо нулем, либо простым числом.*

Доказательство. Пусть n — ненулевая характеристика поля P и $n = p \cdot q$, где p — простое число. Докажем, что для любого x из P имеет место $px = 0$.

Пусть в $P \setminus \{0\}$ имеется такой элемент z, что $pz = 0$.

Умножим обе части последнего равенства на z^{-1}. Получим $p1 = 0$, откуда $p = n$, так как

II.6. Теорема о простоте ненулевой характеристики поля

Теорема 4 (**о простоте ненулевой характеристики поля**). *Характеристика поля является либо нулем, либо простым числом.*

Доказательство. Пусть n — ненулевая характеристика поля P и $n = p \cdot q$, где p — простое число. Докажем, что для любого x из P имеет место $px = 0$.

Пусть в $P \setminus \{0\}$ имеется такой элемент z, что $pz = 0$.

Умножим обе части последнего равенства на z^{-1}. Получим $p1 = 0$, откуда $p = n$, так как по определению характеристики поля n — минимальное число со свойством $n1 = 0$.

II.6. Теорема о простоте ненулевой характеристики поля

Теорема 4 (**о простоте ненулевой характеристики поля**). *Характеристика поля является либо нулем, либо простым числом.*

Доказательство. Пусть n — ненулевая характеристика поля P и $n = p \cdot q$, где p — простое число. Докажем, что для любого x из P имеет место $px = 0$.

Значит, для любого z из $P \setminus \{0\}$ имеем $pz \neq 0$. Возьмем произвольный элемент x из $P \setminus \{0\}$. Тогда $0 = pqx = q(px)$. Введем обозначение: $y = px$. Тогда $qy = 0$. Умножим обе части этого равенства на y^{-1}, получим

II.6. Теорема о простоте ненулевой характеристики поля

Теорема 4 (о простоте ненулевой характеристики поля). *Характеристика поля является либо нулем, либо простым числом.*

Доказательство. Пусть n — ненулевая характеристика поля P и $n = p \cdot q$, где p — простое число. Докажем, что для любого x из P имеет место $px = 0$.

Значит, для любого z из $P \setminus \{0\}$ имеем $pz \neq 0$. Возьмем произвольный элемент x из $P \setminus \{0\}$. Тогда $0 = pqx = q(px)$. Введем обозначение: $y = px$. Тогда $qy = 0$. Умножим обе части этого равенства на y^{-1}, получим $q1 = 0$. По условию $q < n$, что противоречит минимальности n.

Теорема доказана.

II.7. Теорема о цикличности мультипликативной группы поля Галуа

Мы в этом курсе будем рассматривать только **конечные поля**, то есть поля с конечным носителем. Такое поле называется **полем Галуа**.

II.7. Теорема о цикличности мультипликативной группы поля Галуа

Теорема 5. ***Мультипликативная группа*** *поля Галуа P является* ***циклической****, т.е. найдется элемент a такой, что всякий ненулевой элемент поля имеет вид a^k для некоторого неотрицательного целого числа k.*

Доказательство.

II.7. Теорема о цикличности мультипликативной группы поля Галуа

Теорема 5. ***Мультипликативная группа*** *поля Галуа P является* ***циклической****.*

Доказательство. Пусть порядок поля P равен $n+1$ (то есть в множестве P ровно $n+1$ элемент): $P = \{0, a_1, a_2, \ldots, a_n\}$. Пусть в группе $\langle P \setminus \{0\}, \{*, 1\}\rangle$ a_1 — элемент наибольшего порядка m.

Покажем, что всякий элемент поля P является корнем многочлена $x^m - 1$.

II.7. Теорема о цикличности мультипликативной группы поля Галуа

Теорема 5. ***Мультипликативная группа*** *поля Галуа P является* ***циклической***.

Доказательство. $|P| = n + 1$, a_1 — элемент наибольшего порядка m.

Покажем, что всякий элемент поля P является корнем многочлена $x^m - 1$.

Пусть элемент y из $P \setminus \{0\}$ не является корнем этого многочлена. Тогда $y^m \neq 1$. Так как m не делится на $|y|$, то для некоторого простого числа q имеем $m = u * q^s$, $|y| = v * q^t$, $s < t$, числа u и q взаимно просты. Обозначим через z элемент y^v.

II.7. Теорема о цикличности мультипликативной группы поля Галуа

Теорема 5. ***Мультипликативная группа*** *поля Галуа P является* ***циклической***.

Доказательство. $|P| = n + 1$, a_1 — элемент наибольшего порядка m.

Покажем, что всякий элемент поля P является корнем многочлена $x^m - 1$. Пусть $y^m \neq 1$, q — такое простое число, что $m = u * q^s$, $|y| = v * q^t$, $s < t$, числа u и q взаимно просты, $z = y^v$. В силу леммы о делимости на порядок элемента $|z| = q^t$. Пусть $|a_1 * z| = k$. Тогда $a_1^k = (z^{(-1)})^k$. Следовательно, поскольку $|z| = |z^{(-1)}|$, то, по лемме о делимости на порядок элемента, порядок элемента $(z^{(-1)})^k$ равен q^r. Значит, k делится на u: $k = u * w$.

II.7. Теорема о цикличности мультипликативной группы поля Галуа

Теорема 5. ***Мультипликативная группа*** *поля Галуа P является* ***циклической***.

Доказательство. $|P| = n + 1$, a_1 — элемент наибольшего порядка m.

Покажем, что всякий элемент поля P является корнем многочлена $x^m - 1$. Пусть $y^m \neq 1$, q — такое простое число, что $m = u * q^s$, $|y| = v * q^t$, $s < t$, числа u и q взаимно просты, $z = y^v$, $|z| = q^t$.

Итак, если $|a_1 * z| = k$, то k делится на u: $k = u * w$. С другой стороны, по лемме о делимости на порядок элемента, $\left|(a_1 * z)^{(q^s)}\right| = u * q^{(t-s)}$, поэтому рассуждением «от противного» легко получить, что k делится и на q^t.

II.7. Теорема о цикличности мультипликативной группы поля Галуа

Теорема 5. ***Мультипликативная группа*** *поля Галуа P является* ***циклической***.

Доказательство. $|P| = n + 1$, a_1 — элемент наибольшего порядка m.

Покажем, что всякий элемент поля P является корнем многочлена $x^m - 1$. Пусть $y^m \neq 1$, q — такое простое число, что $m = u * q^s$, $|y| = v * q^t$, $s < t$, числа u и q взаимно просты, $z = y^v$, $|z| = q^t$.

Итак, если $|a_1 * z| = k$, то k делится на u: $k = u * w$. С другой стороны, по лемме о делимости на порядок элемента, $\left|(a_1 * z)^{(q^s)}\right| = u * q^{(t-s)}$, поэтому рассуждением «от противного» легко получить, что k делится и на q^t.

Таким образом, k делится на число $u * q^t$, большее m, что противоречит максимальности m.

II.7. Теорема о цикличности мультипликативной группы поля Галуа

Теорема 5. ***Мультипликативная группа*** *поля Галуа P является* ***циклической***.

Доказательство. $|P| = n + 1$, $P = \{0, a_1, a_2, \ldots, a_n\}$, a_1 — элемент наибольшего порядка m. Доказано, что каждый ненулевой элемент поля P является корнем многочлена $x^m - 1$. С помощью математической индукции получаем, что $(x - a_1) * (x - a_2) * \ldots * (x - a_n)$ делится на $x^m - 1$.

II.7. Теорема о цикличности мультипликативной группы поля Галуа

Теорема 5. ***Мультипликативная группа*** *поля Галуа P является* ***циклической***.

Доказательство. $|P| = n + 1, \quad P = \{0, a_1, a_2, \ldots, a_n\}, \quad a_1$ — элемент наибольшего порядка m. Доказано, что каждый ненулевой элемент поля P является корнем многочлена $x^m - 1$.С помощью математической индукции получаем, что $(x - a_1) * (x - a_2) * \ldots * (x - a_n)$ делится на $x^m - 1$. С другой стороны, степень многочлена $(x - a_1) * (x - a_2) * \ldots * (x - a_n)$ равна n и не меньше m. Следовательно,

II.7. Теорема о цикличности мультипликативной группы поля Галуа

Теорема 5. ***Мультипликативная группа*** *поля Галуа P является* ***циклической***.

Доказательство. $|P| = n + 1$, $P = \{0, a_1, a_2, \ldots, a_n\}$, a_1 — элемент наибольшего порядка m. Доказано, что каждый ненулевой элемент поля P является корнем многочлена $x^m - 1$. С помощью математической индукции получаем, что $(x - a_1) * (x - a_2) * \ldots * (x - a_n)$ делится на $x^m - 1$. С другой стороны, степень многочлена $(x - a_1) * (x - a_2) * \ldots * (x - a_n)$ равна n и не меньше m. Следовательно, $m = n$ и $x^n - 1 = (x - a_1) * (x - a_2) * \ldots * (x - a_n)$.

II.7. Теорема о цикличности мультипликативной группы поля Галуа

Теорема 5. ***Мультипликативная группа*** *поля Галуа P является* ***циклической***.

Доказательство. $|P| = n+1$, $P = \{0, a_1, a_2, \ldots, a_n\}$, a_1 — элемент наибольшего порядка m. Доказано, что каждый ненулевой элемент поля P является корнем многочлена $x^m - 1$. С помощью математической индукции получаем, что $(x-a_1) * (x-a_2) * \ldots * (x-a_n)$ делится на $x^m - 1$. С другой стороны, степень многочлена $(x-a_1) * (x-a_2) * \ldots * (x-a_n)$ равна n и не меньше m. Следовательно, $m = n$ и $x^n - 1 = (x-a_1) * (x-a_2) * \ldots * (x-a_n)$.

С другой стороны, для любого k элемент a_1^k является корнем многочлена $x^m - 1$. Значит, $\{a_1, a_2, \ldots, a_n\} = \{a_1, a_1^2, \ldots, a_1^n\}$.

Теорема доказана. **Рассмотрим пример?**

III. Расширения полей

Пусть P — подполе поля F. Тогда F называется **расширением поля** P. Говорят, что поле F получено **присоединением элементов** $s_1, s_2, \ldots, s_n$ к полю P (пишут $F = P(s_1, s_2, \ldots, s_n)$), если в F нет собственных подполей, содержащих одновременно все элементы поля P и элементы $s_1, s_2, \ldots, s_n$.

III. Расширения полей

Пусть P — подполе поля F. Тогда F называется **расширением поля** P. Говорят, что поле F получено **присоединением элементов** $s_1, s_2, \ldots, s_n$ к полю P (пишут $F = P(s_1, s_2, \ldots, s_n)$), если в F нет собственных подполей, содержащих одновременно все элементы поля P и элементы $s_1, s_2, \ldots, s_n$.

Если поле F получено присоединением одного элемента к полю P, то поле F называется **простым расширением поля** P. Подполе P поля F называется **собственным**, если оно отлично от F. Поле P называется **простым**, если оно не содержит собственных подполей.

III.1. Теорема о надполе, как линейном пространстве

Теорема 6 (**о надполе, как линейном пространстве**). *Пусть F — расширение поля P, полученное присоединением элементов $s_1, s_2, \ldots, s_n$, то есть $F = P(s_1, s_2, \ldots, s_n)$. В поле F определена операция сложения элементов, и операция умножения на элементы поля P. Относительно этих операций поле F является линейным пространством над полем P.*

Доказательство сводится к легкой проверке выполнения аксиом линейного пространства.

III.2. Алгебраические и трансцендентные расширения

Если расширение $F = P(s_1, s_2, \ldots, s_n)$ поля P имеет конечную размерность d, как линейное пространство над P, то поле F называется **конечным расширением поля** P, и число d называется **степенью расширения** F поля P. В противном случае говорят, что F - расширение поля P **бесконечной степени**.

III.2. Алгебраические и трансцендентные расширения

Если расширение $F = P(s_1, s_2, \ldots, s_n)$ поля P имеет конечную размерность d, как линейное пространство над P, то поле F называется **конечным расширением поля** P, и число d называется **степенью расширения** F поля P. В противном случае говорят, что F - расширение поля P **бесконечной степени**.

Пусть поле F является расширением поля P. Элемент f поля F называется **алгебраическим над полем** P, если степень поля $P(f)$ над полем P — конечная. В противном случае элемент f называется **трансцендентным над полем** P.

III.2. Алгебраические и трансцендентные расширения

Если расширение $F = P(s_1, s_2, \ldots, s_n)$ поля P имеет конечную размерность d, как линейное пространство над P, то поле F называется **конечным расширением поля** P, и число d называется **степенью расширения** F поля P. В противном случае говорят, что F - расширение поля P **бесконечной степени**.

Пусть поле F является расширением поля P. Элемент f поля F называется **алгебраическим над полем** P, если степень поля $P(f)$ над полем P — конечная. В противном случае элемент f называется **трансцендентным над полем** P.

Если расширение F поля P называется **алгебраическим**, если все элементы поля F являются алгебраическими над P.

III.3. Критерий алгебраичности элемента

Теорема 7 (**критерий алгебраичности элемента**). *Элемент s является алгебраическим над полем P тогда и только тогда, когда s является корнем некоторого ненулевого многочлена с коэффициентами из P, то есть тогда и только тогда, когда для некоторых $a_0, \dots a_m$ из P, не все из которых равны 0 имеем*

$$a_0\mathbf{1} + a_1 s + a_2 s^2 + \ldots + a_m s^m = \mathbf{0},$$

причем m — степень расширения поля $P(s)$ над полем P. Более того, система $\left\{s^0;\ s;\ \ldots;\ s^{m-1}\right\}$ является базисом линейного пространства $P(s)$ над полем P.

Рассмотреть пример?

III.3. Критерий алгебраичности элемента

Доказательство необходимости. Пусть s является алгебраическим над полем P. Обозначим через m размерность линейного пространства $P(s)$ над полем P. Тогда система векторов $\{1, s, s^2, \ldots, s^m\}$ является линейно зависимой, так как

III.3. Критерий алгебраичности элемента

Доказательство необходимости. Пусть s является алгебраическим над полем P. Обозначим через m размерность линейного пространства $P(s)$ над полем P. Тогда система векторов $\{1, s, s^2, \ldots, s^m\}$ является линейно зависимой, так как в ней $m+1$ вектор. Следовательно, в P существуют такие элементы $a_0, \ldots a_m$, не все из которых равны 0, имеем

III.3. Критерий алгебраичности элемента

Доказательство необходимости. Пусть s является алгебраическим над полем P. Обозначим через m размерность линейного пространства $P(s)$ над полем P. Тогда система векторов $\left\{1, s, s^2, \ldots, s^m\right\}$ является линейно зависимой, так как в ней $m+1$ вектор. Следовательно, в P существуют такие элементы $a_0, \ldots a_m$, не все из которых равны 0, имеем

$$a_0\mathbf{1} + a_1 s + a_2 s^2 + \ldots + a_m s^m = \mathbf{0}.$$

Необходимость доказана.

III.3. Критерий алгебраичности элемента

Теорема 7 (**критерий алгебраичности элемента**). *Элемент s является алгебраическим над полем P тогда и только тогда, когда s является корнем некоторого ненулевого многочлена с коэффициентами из P, то есть тогда и только тогда, когда для некоторых $a_0, \dots a_m$ из P, не все из которых равны 0 имеем*

$$a_0\mathbf{1} + a_1 s + a_2 s^2 + \dots + a_m s^m = \mathbf{0},$$

причем m — степень расширения поля $P(s)$ над полем P. Более того, система $\left\{s^0;\ s;\ \dots;\ s^{m-1}\right\}$ является базисом линейного пространства $P(s)$ над полем P.

Достаточность.

III.3. Критерий алгебраичности элемента

Достаточность. Пусть s является корнем многочлена $q(x)$ степени m. Выберем такой многочлен $q(x)$, степень которого минимальна среди всех многочленов с коэффициентами из P, корнем которых является s. Тогда, выражая s^m из уравнения $q(s) = 0$, получаем, что s^m является линейной комбинацией элементов $1, s, s^2, \ldots, s^{m-1}$. Индукцией по $k \geq m$ легко показать, что s^k является линейной комбинацией элементов $1, s, s^2, \ldots, s^{m-1}$.

III.3. Критерий алгебраичности элемента

Достаточность. Индукцией по $k \geq m$ легко показать, что s^k является линейной комбинацией элементов $1, s, s^2, \ldots, s^{m-1}$.

Заметим, что

$$P(s) = \left\{ a_1 + a_2 * s + \ldots + a_m * s^{m-1} \,\middle|\, m \in \mathbb{N}, a_i \in P \right\}.$$

Действительно, обозначим множество в правой части равенства через Q.

III.3. Критерий алгебраичности элемента

Достаточность. Индукцией по $k \geq m$ легко показать, что s^k является линейной комбинацией элементов $1, s, s^2, \ldots, s^{m-1}$.

Заметим, что

$$P(s) = \left\{ a_1 + a_2 * s + \ldots + a_m * s^{m-1} \,\middle|\, m \in \mathbb{N}, a_i \in P \right\}.$$

Действительно, обозначим множество в правой части равенства через Q. Необходимо доказать равенство множеств: $P(s) = Q$. Включение множества Q в $P(s)$ очевидно, так как $P(s)$ — поле, и, следовательно, содержит и элементы вида $a_i * s^i$ для любого неотрицательного целого числа i, и сумму таких элементов. Осталось доказать обратное включение. Для этого необходимо только проверить, что Q — это поле, так как в этом случае $P(s)$ включается в Q в силу минимальности $P(s)$ среди всех полей, содержащих P и s (тот факт, что в P и $\{s\}$ являются подмножествами в Q, очевиден).

III.3. Критерий алгебраичности элемента

Достаточность. Индукцией по $k \geq m$ легко показать, что s^k является линейной комбинацией элементов $1, s, s^2, \ldots, s^{m-1}$.

Заметим, что

$$P(s) = \left\{ a_1 + a_2 * s + \ldots + a_m * s^{m-1} \,\middle|\, m \in \mathbb{N}, a_i \in P \right\}.$$

Действительно, обозначим множество в правой части равенства через Q. Необходимо доказать равенство множеств: $P(s) = Q$.

Итак, осталось доказать, что Q — поле. Неочевидным является только то, что в Q содержится обратный к любому ненулевому элементу из Q. Пусть r — произвольный ненулевой элемент из Q. Докажем, что $\left\{ r, s * r, \ldots, s^{m-1} * r \right\}$ является линейно независимой системой векторов в линейном пространстве $P(s)$.

III.3. Критерий алгебраичности элемента

Достаточность. Пусть r — произвольный ненулевой элемент из Q. Докажем, что $\left\{r, s * r, \ldots, s^{m-1} * r\right\}$ является линейно независимой системой векторов в линейном пространстве $P(s)$. Пусть это не так, тогда $b_1 * r + b_2 * s * r + \ldots + b_m * s^{m-1} * r = 0$, причем не все коэффициенты $b_1, b_2, \ldots, b_m$ равны 0. Вынесем r за скобку, получим, что s является корнем многочлена $r * (b_1 + b_2 * x + \ldots + b_m * x^{m-1})$. Таким образом, s является корнем многочлена r или $b_1 + b_2 * x + \ldots + b_m * x^{m-1}$. Но степень этого многочлена меньше m, что противоречит минимальности m.

III.3. Критерий алгебраичности элемента

Достаточность. Пусть r — произвольный ненулевой элемент из Q. Доказано, что $\left\{r, s * r, \ldots, s^{m-1} * r\right\}$ — линейно независимая система векторов. Как доказано выше, для любого $k \geq m$ элемент s^k является линейной комбинацией элементов $1, s, \ldots, s^{m-1}$. Поэтому каждый из $s^k * r$ представим в виде значения многочлена степени, меньшей m, на элементе s, то есть $s^k * r$ является элементом из Q. Размерность Q, как линейного пространства над P, равна m, следовательно, $\left\{r, s * r, \ldots, s^{m-1} * r\right\}$ является базисом линейного пространства Q. В частности, элемент 1 представим в виде

$$1 = c_0 * r + c_1 * s * r + \ldots + c_m * s^{m-1} * r =$$

$$= r * (c_0 + c_1 * s + \ldots + c_m * s^{m-1}).$$

III.3. Критерий алгебраичности элемента

Достаточность. Пусть r — произвольный ненулевой элемент из Q. Доказано, что $\left\{r, s * r, \ldots, s^{m-1} * r\right\}$ — линейно независимая система векторов, являющаяся базисом линейного пространства Q.

$$1 = c_0 * r + c_1 * s * r + \ldots + c_m * s^{m-1} * r =$$

$$= r * (c_0 + c_1 * s + \ldots + c_m * r^{m-1}).$$

Таким образом, $c_0 + c_1 * s + \ldots + c_m * r^{m-1}$ является обратным элементом к r относительно умножения. Следовательно, Q — это поле, поэтому $Q = P(s)$. Но размерность Q, как линейного пространства над P, равна m, то есть $P(s)$ — алгебраическое расширение.

III.4. Теорема о степенях

Теорема 8 (о степенях). *Если поле Q конечно над P, и поле T конечно над Q, то поле T конечно и над P, причем размерность линейного пространства T над полем P равна $n \cdot m$, где n — размерность линейного пространства Q над P, и m — размерность линейного пространства T над Q.*

III.4. Теорема о степенях

Теорема 8 (о степенях). *Если поле Q конечно над P, и поле T конечно над Q, то поле T конечно и над P, причем размерность линейного пространства T над полем P равна $n \cdot m$, где n — размерность линейного пространства Q над P, и m — размерность линейного пространства T над Q.*

Доказательство. Пусть $\{u_1, u_2, \ldots, u_n\}$ — базис линейного пространства Q над полем P, $\{v_1, \ldots, v_m\}$ - базис линейного пространства T над полем Q. Каждый элемент из T представим в виде $b_1 * v_1 + \ldots + b_m * v_m$, где $b_1, b_2, \ldots, b_m$ — элементы из Q. По теореме о линейных комбинациях базисных векторов получаем (курс алгебры, первый и третий семестры), что

III.4. Теорема о степенях

Теорема 8 (**о степенях**). *Если поле Q конечно над P, и поле T конечно над Q, то поле T конечно и над P, причем размерность линейного пространства T над полем P равна $n \cdot m$, где n — размерность линейного пространства Q над P, и m — размерность линейного пространства T над Q.*

Доказательство. $b_1 * v_1 + \ldots + b_m * v_m$

$$\begin{cases} b_1 = a_{11} * u_1 + \ldots + a_{1n} * u_n \\ b_2 = a_{21} * u_1 + \ldots + a_{2n} * u_n \\ \ldots \\ b_m = a_{m1} * u_1 + \ldots + a_{mn} * u_n \end{cases}$$

Следовательно,

III.4. Теорема о степенях

Теорема 8 (**о степенях**). *Если поле Q конечно над P, и поле T конечно над Q, то поле T конечно и над P, причем размерность линейного пространства T над полем P равна $n \cdot m$, где n — размерность линейного пространства Q над P, и m — размерность линейного пространства T над Q.*

Доказательство.

$$b_1 * v_1 + \ldots + b_m * v_m =$$

$$= (a_{11} * u_1 + \ldots + a_{1n} * u_n) * v_1 + \ldots + (a_{m1} * u_1 + \ldots + a_{mn} * u_n) * v_m =$$

$$= a_{11} * u_1 * v_1 + \ldots + a_{1n} * u_n * v_1 + \ldots + a_{m1} * u_1 * v_m + \ldots + a_{mn} * u_n * v_m.$$

III.4. Теорема о степенях

Теорема 8 (**о степенях**). *Если поле Q конечно над P, и поле T конечно над Q, то поле T конечно и над P, причем размерность линейного пространства T над полем P равна $n \cdot m$, где n — размерность линейного пространства Q над P, и m — размерность линейного пространства T над Q.*

Доказательство. Таким образом, система векторов

$$\{u_1 * v_1, \ldots, u_n * v_1, \ldots, u_1 * v_m, \ldots, u_n * v_m\}$$

полна, то есть любой вектор представим в виде их линейной комбинации. Очевидно, что эта система линейно независима, иначе получили бы линейную зависимость системы $\{v_1, v_2, \ldots, v_m\}$. Теорема доказана.

III.5. Критерий конечности расширения поля

Теорема 9 (**критерий конечности расширения поля** P). *Пусть поле F является расширением поля P с помощью элементов $s_1, s_2, \ldots, s_n$. Тогда поле F является конечным расширением поля P тогда и только тогда, когда $s_1, s_2, \ldots, s_n$ являются корнями некоторых многочленов $q_1(x), q_2(x), \ldots, q_n(x)$ с коэффициентами из поля P.*

Доказательство. Это следствие из критерия алгебраичности элемента и теоремы о степенях.

III.6. Следствие об алгебраичности конечного расширения поля

Следствие 1. *Если F — **конечное расширение** поля P, то оно является **алгебраическим** над P.*

Доказательство.

III.6. Следствие об алгебраичности расширения поля

Следствие 1. *Если F — **конечное расширение** поля P, то оно является **алгебраическим** над P.*

Доказательство. С чего начнем доказательство?

III.6. Следствие об алгебраичности расширения поля

Следствие 1. *Если F — **конечное расширение** поля P, то оно является **алгебраическим** над P.*

Доказательство. Пусть F — **конечное расширение** поля P и $a \in F$.

III.6. Следствие об алгебраичности расширения поля

Следствие 1. *Если F — **конечное расширение** поля P, то оно является **алгебраическим** над P.*

Доказательство. Пусть F — **конечное расширение** поля P и $a \in F$.

Тогда согласно **критерию конечности расширения поля** элемент a является корнем многочлена с коэффициентами из P, т.е. является алгебраическим над P.

III.6. Следствие об алгебраичности расширения поля

Следствие 1. *Если F — **конечное расширение** поля P, то оно является **алгебраическим** над P.*

Доказательство. Пусть F — **конечное расширение** поля P и $a \in F$.

Тогда согласно **критерию конечности расширения поля** элемент a является корнем многочлена с коэффициентами из P, т.е. является алгебраическим над P.

Значит, расширение F является алгебраическим над P. Следствие доказано.

III.7. Следствие о порядке простого конечного поля

Следствие 2 (**о порядке простого конечного поля**). *Конечное поле является простым тогда и только тогда, когда количество элементов поля P — простое число.*

Доказательство необходимости.

III.7. Следствие о порядке простого конечного поля

Следствие 2 (**о порядке простого конечного поля**). *Конечное поле является простым тогда и только тогда, когда количество элементов поля P — простое число.*

Доказательство необходимости. Пусть P — простое конечное поле характеристики p. Тогда, очевидно, в силу теоремы о характеристике поля, $\langle 1, 1+1, \ldots, p*1\rangle$ — подполе в P, и, в силу простоты поля P имеем $P = \langle 1, 1+1, \ldots, p*1\rangle$, в частности, его порядок равен p. Необходимость доказана, так как, по теореме о простоте ненулевой характеристики поля, p — простое число

III.7. Следствие о порядке простого конечного поля

Следствие 2 (**о порядке простого конечного поля**). *Конечное поле является простым тогда и только тогда, когда количество элементов поля P — простое число.*

Достаточность. Пусть $|P| = p$ — простое число. Аддитивная группа любого подполя Q поля P является подгруппой аддитивной группы поля P. По теореме Лагранжа ее порядок делится на $|P| = p$, но у простого числа нет неединичных собственных делителей. Следовательно, $|Q| = |P|$, откуда следует, что $P = Q$, что и требовалось доказать. Следствие доказано.

III.8. Следствие о порядке конечного поля

Следствие 3 (**о порядке конечного поля**). *Конечное поле содержит p^t элементов, где p — простое число, t — неотрицательное целое число.*

Доказательство. Пусть характеристика поля P равна p (она, очевидно, не нулевая). Доказательство будем вести индукцией по порядку поля.

III.8. Следствие о порядке конечного поля

Следствие 3 (**о порядке конечного поля**). *Конечное поле содержит p^t элементов, где p — простое число, t — неотрицательное целое число.*

Доказательство. *База индукции.* Если поле P — простое, то заключение теоремы вытекает из предыдущего следствия.

III.8. Следствие о порядке конечного поля

Следствие 3 (о порядке конечного поля). *Конечное поле содержит p^t элементов, где p — простое число, t — неотрицательное целое число.*

Доказательство. *Шаг индукции.* Пусть конечное поле P — не простое. Выберем в нем максимальное собственное подполе Q. Возьмем элемент z из $P \backslash Q$. Тогда расширение $Q(z)$ поля Q с помощью элемента z совпадает с P, в силу максимальности подполя Q в P. Пусть m — максимальное такое число, что $\mathbf{Б} = \{1, z, \ldots, z^m\}$ — линейно независимая система векторов. Тогда, очевидно, $\mathbf{Б}$ — это базис P, как линейного пространства над Q.

III.8. Следствие о порядке конечного поля

Следствие 3 (о порядке конечного поля). *Конечное поле содержит p^t элементов, где p — простое число, t — неотрицательное целое число.*

Доказательство. Q — максимальное собственное подполе поля P, $z \in P \backslash Q$, $Q(z) = P$, $\mathbf{Б} = \{1, z, \ldots, z^m\}$ — это базис P, как линейного пространства над Q.

Каждая координата любого вектора из P принимает ровно p значений $\{0, 1, \ldots, p-1\}$, так $px = 0$ для любого x из P. Как доказывалось в линейной алгебре, линейное конечномерное пространство изоморфно линейному пространству матриц-столбцов размерности, в данном случае, $m+1$. Значит $|P| = |Q|^{m+1}$, но, по предположению индукции $|Q| = p^s$, следовательно, $|P| = p^t$, где $t = s * (m+1)$. Следствие доказано.

III.9. Теорема о степени многочлена для конечного расширения

Теорема 10 (**о степени многочлена для конечного расширения**). *Если поле F является конечным расширением поля P, и степень расширения F поля P равна n, то любой элемент поля F является корнем многочлена степени не большей n, с коэффициентами из поля P.*

Доказательство.

III.9. Теорема о степени многочлена для конечного расширения

Теорема 10 (о степени многочлена для конечного расширения). *Если поле F является конечным расширением поля P, и степень расширения F поля P равна n, то любой элемент поля F является корнем многочлена степени не большей n, с коэффициентами из поля P.*

Доказательство. Возьмем произвольный элемент a из поля F. По условию размерность F, как линейного пространства над P, равна n. Значит, система векторов $\left\{1, a, a * a, a^3, \ldots, a^n\right\}$ является линейно зависимой. Таким образом, для некоторых элементов $b_0, b_1, \ldots, b_n$ поля P имеет место равенство $b_0 * 1 + b_1 * a + \ldots + b_n * a^n = 0$, то есть a является корнем многочлена $b_0 * 1 + b_1 * x + \ldots + b_n * x^n$, что и требовалось доказать.

IV. Поле частных целостного кольца

Пусть K — коммутативное **целостное кольцо**. Рассмотрим множество «дробей»

$$K' = \left\{ \frac{p}{q} \middle| p, q \in K, q \neq 0 \right\}.$$

IV.1. Операции кольца частных

Пусть K — коммутативное **целостное кольцо**. Рассмотрим множество «дробей»

$$K' = \left\{ \frac{p}{q} \middle| p, q \in K, q \neq 0 \right\}.$$

На множестве K' определим операции сложения и умножения, аналогичные операциям для обычных дробей и для дробно-рациональных функций:

IV.1. Операции кольца частных

Пусть K — коммутативное **целостное кольцо**. Рассмотрим множество «дробей»

$$K' = \left\{ \frac{p}{q} \middle| p, q \in K, q \neq 0 \right\}.$$

На множестве K' определим операции сложения и умножения, аналогичные операциям для обычных дробей и для дробно-рациональных функций:

$$\frac{p}{q} + \frac{u}{v} = \frac{p * v + q * u}{q * v}, \quad \text{и}$$

IV.1. Операции кольца частных

Пусть K — коммутативное **целостное кольцо**. Рассмотрим множество «дробей»

$$K' = \left\{ \frac{p}{q} \middle| p, q \in K, q \neq 0 \right\}.$$

На множестве K' определим операции сложения и умножения, аналогичные операциям для обычных дробей и для дробно-рациональных функций:

$$\frac{p}{q} + \frac{u}{v} = \frac{p * v + q * u}{q * v}, \quad \text{и} \quad \frac{p}{q} * \frac{u}{v} = \frac{p * u}{q * v}.$$

IV.2. Лемма о конгруенции кольца частных

Лемма 1. *Пусть* ***бинарное отношение*** T *определено на множестве* K' *правилом:* $\left(\frac{a}{b};\frac{c}{d}\right) \in T$ *тогда и только тогда, когда* $a * d = b * c$. *Тогда* T *является* ***конгруенцией***.

Фу-у-у, какая громоздкая формулировка...

IV.2. Лемма о конгруенции кольца частных

Лемма 1. *Если*

$$\left(\frac{a}{b};\frac{c}{d}\right) \in T \;\Leftrightarrow\; a * d = b * c, \tag{2}$$

то T является ***конгруенцией****.*

Доказательство. По **определению конгруенции** надо проверить, что T является **отношением эквивалентности**, и что

IV.2. Лемма о конгруенции кольца частных

Лемма 1. *Если*

$$\left(\frac{a}{b};\frac{c}{d}\right) \in T \;\Leftrightarrow\; a * d = b * c, \tag{2}$$

то T является ***конгруенцией****.*

Доказательство. По **определению конгруенции** надо проверить, что T является **отношением эквивалентности**, и что

(подставим в **формулу** в качестве операции f операцию «сложение»)

IV.2. Лемма о конгруенции кольца частных

Лемма 1. *Если*

$$\left(\frac{a}{b};\frac{c}{d}\right) \in T \;\Leftrightarrow\; a * d = b * c, \tag{2}$$

то T является ***конгруенцией****.*

Доказательство. По **определению конгруенции** надо проверить, что T является **отношением эквивалентности**, и что

$$\begin{cases} (x_1,\ y_1) \in T, \\ (x_2,\ y_2) \in T \end{cases} \Rightarrow$$

IV.2. Лемма о конгруенции кольца частных

Лемма 1. *Если*

$$\left(\frac{a}{b};\frac{c}{d}\right) \in T \;\Leftrightarrow\; a * d = b * c, \tag{2}$$

то T является ***конгруенцией****.*

Доказательство. По **определению конгруенции** надо проверить, что T является **отношением эквивалентности**, и что

$$\begin{cases} (x_1,\ y_1) \in T, \\ (x_2,\ y_2) \in T \end{cases} \Rightarrow\ (x_1 + x_2,\ y_1 + y_2) \in T,$$

IV.2. Лемма о конгруенции кольца частных

Лемма 1. *Если*

$$\left(\frac{a}{b};\frac{c}{d}\right)\in T \;\Leftrightarrow\; a*d=b*c, \tag{2}$$

то T является ***конгруенцией****.*

Доказательство. По **определению конгруенции** надо проверить, что T является **отношением эквивалентности**, и что

$$\begin{cases}(x_1,\ y_1)\in T,\\ (x_2,\ y_2)\in T\end{cases}\ \Rightarrow\ (x_1+x_2,\ y_1+y_2)\in T,$$

(теперь подставим в **формулу** в качестве операции f «операцию умножение»)

IV.2. Лемма о конгруенции кольца частных

Лемма 1. *Если*

$$\left(\frac{a}{b};\frac{c}{d}\right) \in T \;\Leftrightarrow\; a * d = b * c, \tag{2}$$

то T является ***конгруенцией****.*

Доказательство. По **определению конгруенции** надо проверить, что T является **отношением эквивалентности**, и что

$$\begin{cases} (x_1,\ y_1) \in T, \\ (x_2,\ y_2) \in T \end{cases} \Rightarrow\ (x_1 + x_2,\ y_1 + y_2) \in T,$$

$$\begin{cases} (x_1,\ y_1) \in T, \\ (x_2,\ y_2) \in T \end{cases} \Rightarrow$$

IV.2. Лемма о конгруенции кольца частных

Лемма 1. *Если*

$$\left(\frac{a}{b};\frac{c}{d}\right)\in T \;\Leftrightarrow\; a*d=b*c, \tag{2}$$

то T является ***конгруенцией****.*

Доказательство. По **определению конгруенции** надо проверить, что T является **отношением эквивалентности**, и что

$$\begin{cases}(x_1,\ y_1)\in T,\\ (x_2,\ y_2)\in T\end{cases}\Rightarrow\ (x_1+x_2,\ y_1+y_2)\in T,$$

$$\begin{cases}(x_1,\ y_1)\in T,\\ (x_2,\ y_2)\in T\end{cases}\Rightarrow\ (x_1*x_2,\ y_1*y_2)\in T.$$

IV.2. Лемма о конгруенции кольца частных

Лемма 1. *Если*

$$\left(\frac{a}{b};\frac{c}{d}\right)\in T \;\Leftrightarrow\; a*d=b*c, \tag{2}$$

то T является ***конгруенцией***.

Доказательство.

$$\begin{cases} \left(\frac{a}{b};\frac{c}{d}\right)\in T, \\ \left(\frac{u}{v};\frac{w}{z}\right)\in T \end{cases} \Rightarrow$$

$$\Rightarrow \left(\frac{a}{b}+\frac{u}{v};\ \frac{c}{d}+\frac{w}{z}\right)\in T.$$

IV.2. Лемма о конгруенции кольца частных

Лемма 1. *Если*

$$\left(\frac{a}{b};\frac{c}{d}\right)\in T \;\Leftrightarrow\; a*d=b*c, \tag{2}$$

то T является ***конгруенцией****.*

Доказательство.

$$\begin{cases} \left(\frac{a}{b};\frac{c}{d}\right)\in T, \\ \left(\frac{u}{v};\frac{w}{z}\right)\in T \end{cases} \Rightarrow$$

$$\Rightarrow \left(\frac{a*v+u*b}{b*v};\ \frac{c*z+w*d}{d*z}\right)\in T \Rightarrow \left(\frac{a}{b}+\frac{u}{v};\ \frac{c}{d}+\frac{w}{z}\right)\in T.$$

IV.2. Лемма о конгруенции кольца частных

Лемма 1. *Если*

$$\left(\frac{a}{b};\frac{c}{d}\right)\in T \;\Leftrightarrow\; a*d=b*c, \tag{2}$$

то T является ***конгруенцией***.

Доказательство.

$$\begin{cases} \left(\frac{a}{b};\frac{c}{d}\right)\in T, \\ \left(\frac{u}{v};\frac{w}{z}\right)\in T \end{cases} \Rightarrow$$

$$\Rightarrow\; (a*v+u*b)*d*z=(c*z+w*d)*b*v \;\Rightarrow$$

$$\Rightarrow\; \left(\frac{a*v+u*b}{b*v};\;\frac{c*z+w*d}{d*z}\right)\in T \;\Rightarrow\; \left(\frac{a}{b}+\frac{u}{v};\;\frac{c}{d}+\frac{w}{z}\right)\in T.$$

IV.2. Лемма о конгруенции кольца частных

Лемма 1. *Если*

$$\left(\frac{a}{b};\frac{c}{d}\right)\in T \;\Leftrightarrow\; a*d=b*c, \tag{2}$$

то T является ***конгруенцией****.*

Доказательство.

$$\begin{cases} \left(\frac{a}{b};\frac{c}{d}\right)\in T, \\ \left(\frac{u}{v};\frac{w}{z}\right)\in T \end{cases} \Rightarrow$$

$$\Rightarrow\; a*v*d*z+u*b*d*z=c*z*b*v+w*d*b*v \;\Rightarrow$$

$$\Rightarrow\; (a*v+u*b)*d*z=(c*z+w*d)*b*v \;\Rightarrow$$

$$\Rightarrow\; \left(\frac{a*v+u*b}{b*v};\;\frac{c*z+w*d}{d*z}\right)\in T \;\Rightarrow\; \left(\frac{a}{b}+\frac{u}{v};\;\frac{c}{d}+\frac{w}{z}\right)\in T.$$

IV.2. Лемма о конгруенции кольца частных

Лемма 1. *Если*

$$\left(\frac{a}{b};\frac{c}{d}\right)\in T \;\Leftrightarrow\; a*d=b*c, \tag{2}$$

то T является ***конгруенцией***.

Доказательство.

$$\left\{\begin{array}{l}\left(\frac{a}{b};\frac{c}{d}\right)\in T,\\ \left(\frac{u}{v};\frac{w}{z}\right)\in T\end{array}\right. \Rightarrow \left\{\begin{array}{l}a*d=b*c,\\ u*z=v*w\end{array}\right. \Rightarrow$$

$$\Rightarrow\; a*v*d*z+u*b*d*z=c*z*b*v+w*d*b*v \;\Rightarrow$$

$$\Rightarrow\; (a*v+u*b)*d*z=(c*z+w*d)*b*v \;\Rightarrow$$

$$\Rightarrow\; \left(\frac{a*v+u*b}{b*v};\;\frac{c*z+w*d}{d*z}\right)\in T \;\Rightarrow\; \left(\frac{a}{b}+\frac{u}{v};\;\frac{c}{d}+\frac{w}{z}\right)\in T.$$

IV.2. Лемма о конгруенции кольца частных

Лемма 1. *Если*

$$\left(\frac{a}{b};\frac{c}{d}\right)\in T \;\Leftrightarrow\; a*d=b*c, \tag{2}$$

то T является ***конгруенцией***.

Доказательство.

$$\begin{cases} \left(\frac{a}{b};\frac{c}{d}\right)\in T, \\ \left(\frac{u}{v};\frac{w}{z}\right)\in T \end{cases} \Rightarrow$$

$$\Rightarrow \left(\frac{a}{b}*\frac{u}{v};\ \frac{c}{d}*\frac{w}{z}\right)\in T.$$

IV.2. Лемма о конгруенции кольца частных

Лемма 1. *Если*

$$\left(\frac{a}{b};\frac{c}{d}\right)\in T \;\Leftrightarrow\; a*d=b*c, \tag{2}$$

то T является ***конгруенцией***.

Доказательство.

$$\begin{cases} \left(\frac{a}{b};\frac{c}{d}\right)\in T, \\ \left(\frac{u}{v};\frac{w}{z}\right)\in T \end{cases} \Rightarrow$$

$$\Rightarrow \left(\frac{a*u}{b*v};\ \frac{c*w}{d*z}\right)\in T \Rightarrow \left(\frac{a}{b}*\frac{u}{v};\ \frac{c}{d}*\frac{w}{z}\right)\in T.$$

IV.2. Лемма о конгруенции кольца частных

Лемма 1. *Если*

$$\left(\frac{a}{b};\frac{c}{d}\right)\in T \;\Leftrightarrow\; a*d=b*c, \tag{2}$$

то T является ***конгруенцией***.

Доказательство.

$$\begin{cases} \left(\frac{a}{b};\frac{c}{d}\right)\in T, \\ \left(\frac{u}{v};\frac{w}{z}\right)\in T \end{cases} \Rightarrow$$

$$\Rightarrow\; a*u*d*z=c*w*b*v \;\Rightarrow$$

$$\Rightarrow\; \left(\frac{a*u}{b*v};\;\frac{c*w}{d*z}\right)\in T \;\Rightarrow\; \left(\frac{a}{b}*\frac{u}{v};\;\frac{c}{d}*\frac{w}{z}\right)\in T.$$

IV.2. Лемма о конгруенции кольца частных

Лемма 1. *Если*

$$\left(\frac{a}{b};\frac{c}{d}\right)\in T \;\Leftrightarrow\; a*d=b*c, \tag{2}$$

то T является ***конгруенцией***.

Доказательство.

$$\left\{\begin{array}{l}\left(\frac{a}{b};\frac{c}{d}\right)\in T,\\ \left(\frac{u}{v};\frac{w}{z}\right)\in T\end{array}\right. \Rightarrow \left\{\begin{array}{l}a*d=b*c,\\ u*z=v*w\end{array}\right. \Rightarrow$$

$$\Rightarrow\; a*u*d*z=c*w*b*v \;\Rightarrow$$

$$\Rightarrow\; \left(\frac{a*u}{b*v};\;\frac{c*w}{d*z}\right)\in T \;\Rightarrow\; \left(\frac{a}{b}*\frac{u}{v};\;\frac{c}{d}*\frac{w}{z}\right)\in T.$$

IV.2. Лемма о конгруенции кольца частных

Лемма 1. *Если*

$$\left(\frac{a}{b};\frac{c}{d}\right)\in T \;\Leftrightarrow\; a*d=b*c, \tag{2}$$

то T является ***конгруенцией***.

Доказательство.

$$\left\{\begin{array}{l}\left(\frac{a}{b};\frac{c}{d}\right)\in T,\\ \left(\frac{u}{v};\frac{w}{z}\right)\in T\end{array}\right. \Rightarrow \left\{\begin{array}{l}a*d=b*c,\\ u*z=v*w\end{array}\right. \Rightarrow$$

$$\Rightarrow\; a*d*u*z=c*b*w*v \;\Rightarrow\; a*u*d*z=c*w*b*v \;\Rightarrow$$

$$\Rightarrow \left(\frac{a*u}{b*v};\;\frac{c*w}{d*z}\right)\in T \;\Rightarrow\; \left(\frac{a}{b}*\frac{u}{v};\;\frac{c}{d}*\frac{w}{z}\right)\in T.$$

IV.2. Лемма о конгруенции кольца частных

Лемма 1. *Если*

$$\left(\frac{a}{b};\frac{c}{d}\right)\in T \;\Leftrightarrow\; a*d=b*c, \tag{2}$$

то T является ***конгруенцией****.*

Доказательство. Итак,

$$\begin{cases} \left(\frac{a}{b};\frac{c}{d}\right)\in T, \\ \left(\frac{u}{v};\frac{w}{z}\right)\in T \end{cases} \Rightarrow \left(\frac{a}{b}+\frac{u}{v};\ \frac{c}{d}+\frac{w}{z}\right)\in T.$$

$$\begin{cases} \left(\frac{a}{b};\frac{c}{d}\right)\in T, \\ \left(\frac{u}{v};\frac{w}{z}\right)\in T \end{cases} \Rightarrow \left(\frac{a}{b}*\frac{u}{v};\ \frac{c}{d}*\frac{w}{z}\right)\in T.$$

Тот факт, что T — **отношение эквивалентности**, очевиден. Следовательно, T — **конгруенция**. Лемма доказана.

IV.3. Теорема о поле частных

Теорема 11. *Если K — коммутативное* ***целостное кольцо****, то алгебра $K'/\mathbf{T}$ является* ***полем****.*

Доказательство.

IV.3. Теорема о поле частных

Теорема 11. *Если K — коммутативное* ***целостное кольцо****, то алгебра $K'/\mathbf{T}$ является* ***полем****.*

Доказательство. Докажем, что $\langle K', \{+, 0\}\rangle$ — абелева группа.

IV.3. Теорема о поле частных

Теорема 11. *Если K — коммутативное* ***целостное кольцо****, то алгебра $K'/\mathbf{T}$ является* ***полем****.*

Доказательство. Докажем, что $\langle K', \{+, 0\}\rangle$ — абелева группа.

Коммутативность и ассоциативность очевидны (проверяются непосредственным вычислением).

IV.3. Теорема о поле частных

Теорема 11. *Если K — коммутативное* ***целостное кольцо****, то алгебра $K'/\mathbf{T}$ является* ***полем****.*

Доказательство. Докажем, что $\langle K', \{+, 0\}\rangle$ — абелева группа.

Коммутативность и ассоциативность очевидны (проверяются непосредственным вычислением). Легко понять, что в качестве обратного относительно $+$ элемента к элементу $\frac{a}{b}$ можно взять $\frac{-a}{b}$.

IV.3. Теорема о поле частных

Теорема 11. *Если K — коммутативное* ***целостное кольцо****, то алгебра $K'/\mathbf{T}$ является* ***полем****.*

Доказательство. Докажем, что $\langle K', \{+, 0\}\rangle$ — абелева группа.

Коммутативность и ассоциативность очевидны (проверяются непосредственным вычислением). Легко понять, что в качестве обратного относительно $+$ элемента к элементу $\frac{a}{b}$ можно взять $\frac{-a}{b}$. Нулевым элементом является класс «дробей» вида $\frac{0}{b}$.

IV.3. Теорема о поле частных

Теорема 11. *Если K — коммутативное* ***целостное кольцо****, то алгебра $K'/\mathbf{T}$ является* ***полем****.*

Доказательство. Проверим, что

$$\left\langle (K'/T) \setminus \left\{ \frac{0}{x} \,\middle|\, x \in K' \right\}, \left\{ *, \left\{ \frac{x}{x} \,\middle|\, x \in K' \right\} \right\} \right\rangle$$

— абелева группа.

IV.3. Теорема о поле частных

Теорема 11. *Если K — коммутативное* ***целостное кольцо****, то алгебра $K'/\mathbf{T}$ является* ***полем****.*

Доказательство. Проверим, что

$$\left\langle (K'/T)\setminus \left\{ \frac{0}{x} \,\middle|\, x \in K' \right\}, \left\{ *, \left\{ \frac{x}{x} \,\middle|\, x \in K' \right\} \right\} \right\rangle$$

— абелева группа. Абелевость легко следует из коммутативности кольца K, ассоциативность очевидна.

IV.3. Теорема о поле частных

Теорема 11. *Если K — коммутативное* ***целостное кольцо****, то алгебра $K'/\mathbf{T}$ является* ***полем****.*

Доказательство. Проверим, что

$$\left\langle (K'/T)\setminus \left\{ \frac{0}{x} \,\middle|\, x \in K' \right\}, \left\{ *, \left\{ \frac{x}{x} \,\middle|\, x \in K' \right\} \right\} \right\rangle$$

— абелева группа. Обратным относительно операции $*$ элементом к ненулевому элементу $\left\{ \frac{x}{y} \,\middle|\, \left(\frac{x}{y};\ \frac{a}{b}\right) \in T \right\}$ для $a \neq 0$ является класс «дробей»

IV.3. Теорема о поле частных

Теорема 11. *Если K — коммутативное* ***целостное кольцо****, то алгебра $K'/\mathbf{T}$ является* ***полем****.*

Доказательство. Проверим, что

$$\left\langle (K'/T)\setminus \left\{ \frac{0}{x} \,\middle|\, x \in K' \right\}, \left\{ *, \left\{ \frac{x}{x} \,\middle|\, x \in K' \right\} \right\} \right\rangle$$

— абелева группа. Обратным относительно операции $*$ элементом к ненулевому элементу $\left\{ \frac{x}{y} \,\middle|\, \left(\frac{x}{y};\ \frac{a}{b}\right) \in T \right\}$ для $a \neq 0$ является класс «дробей» $\left\{ \frac{u}{v} \,\middle|\, \left(\frac{u}{v};\ \frac{b}{a}\right) \in T \right\}$.

IV.3. Теорема о поле частных

Теорема 11. *Если K — коммутативное* ***целостное кольцо****, то алгебра $K'/\mathbf{T}$ является* ***полем****.*

Доказательство. Проверим, что

$$\left\langle (K'/T) \setminus \left\{ \frac{0}{x} \,\middle|\, x \in K' \right\}, \left\{ *, \left\{ \frac{x}{x} \,\middle|\, x \in K' \right\} \right\} \right\rangle$$

— абелева группа.

Проверка дистрибутивности также не вызывает затруднений, мы опустим соответствующие выкладки.

IV.3. Теорема о поле частных

Теорема 11. *Если K — коммутативное* ***целостное кольцо****, то алгебра $K'/\mathbf{T}$ является* ***полем****.*

Теорема доказана.

IV.4. Определение поля частных

Определение 5. *Поле* K'/T *из формулировки* ***теоремы о поле частных*** *называется* **полем частных кольца** K.

IV.4. Определение поля частных

Определение 5. *Поле K'/T из формулировки* ***теоремы о поле частных*** *называется* **полем частных кольца** K.

Отметим, что нами допущена некорректность: символом $*$ (как и символом $+$) обозначены одновременно три операции: в K, в множестве «дробей» K' и в фактор-алгебре K'/T. Это, однако, не вызывает затруднений, поскольку каждый раз из контекста понятно, какая из конкретных операций имеется в виду.

IV.4. Определение поля частных

Определение 5. *Поле K'/T из формулировки* ***теоремы о поле частных*** *называется* **полем частных кольца** K.

Отметим еще два факта.

Во-первых, поле Q рациональных функций является полем частных кольца целых чисел.

IV.4. Определение поля частных

Определение 5. *Поле K'/T из формулировки* ***теоремы о поле частных*** *называется* **полем частных кольца** K.

Отметим еще два факта.

Во-первых, поле Q рациональных функций является полем частных кольца целых чисел.

Во-вторых, кольцо K изоморфно вкладывается в K'/T с помощью правила: элементу a из K поставим в соответствие класс, содержащий $\frac{a}{1}$. Легко проверить (сделайте это самостоятельно), что это отображение является изоморфизмом.

V. Расширение поля с помощью кольца многочленов

Пусть P — **поле**. Через $P[x]$ обозначим алгебру **многочленов** с коэффициентами из P, с обычными операциями сложения многочленов и умножения многочленов. Очевидно, что относительно этих операций $P[x]$ является **кольцом**.

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство.

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть T — **конгруенция**. Перейдем это утверждение на язык подмножеств. Пусть F — **отношение**, определенное формулой $F = \{(a,b) \,|\, a + I = b + I\}$.

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть T — **конгруенция**. Перейдем это утверждение на язык подмножеств. Пусть F — **отношение**, определенное формулой $F = \{(a,b) \,|\, a + I = b + I\}$. Докажем, что $T \subseteq F$. По **определению конгруенции**, если $(a,b) \in T$, то

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть T — **конгруенция**. Перейдем это утверждение на язык подмножеств. Пусть F — **отношение**, определенное формулой $F = \{(a,b) \,|\, a + I = b + I\}$. Докажем, что $T \subseteq F$. По **определению конгруенции**, если $(a,b) \in T$, то

$$\begin{cases} (a;b) \in T, \\ (-a,-a) \in T \end{cases} \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть T — **конгруенция**. Перейдем это утверждение на язык подмножеств. Пусть F — **отношение**, определенное формулой $F = \{(a,b) \,|\, a + I = b + I\}$. Докажем, что $T \subseteq F$. По **определению конгруенции**, если $(a,b) \in T$, то

$$\begin{cases} (a;b) \in T, \\ (-a,-a) \in T \end{cases} \Rightarrow (a-a, b-a) \in T \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть T — **конгруенция**. Перейдем это утверждение на язык подмножеств. Пусть F — **отношение**, определенное формулой $F = \{(a,b) \,|\, a + I = b + I\}$. Докажем, что $T \subseteq F$. По **определению конгруенции**, если $(a,b) \in T$, то

$$\begin{cases} (a;b) \in T, \\ (-a,-a) \in T \end{cases} \Rightarrow (a-a, b-a) \in T \Rightarrow (b-a, 0) \in T \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть T — **конгруенция**. Перейдем это утверждение на язык подмножеств. Пусть F — **отношение**, определенное формулой $F = \{(a,b) \,|\, a + I = b + I\}$. Докажем, что $T \subseteq F$. По **определению конгруенции**, если $(a,b) \in T$, то

$$\begin{cases} (a;b) \in T, \\ (-a,-a) \in T \end{cases} \Rightarrow (a-a, b-a) \in T \Rightarrow (b-a, 0) \in T \Rightarrow (b-a) \in I.$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть T — **конгруенция**. Перейдем это утверждение на язык подмножеств. Пусть F — **отношение**, определенное формулой $F = \{(a,b) \,|\, a + I = b + I\}$. Докажем, что $T \subseteq F$. По **определению конгруенции**, если $(a,b) \in T$, то

$$\begin{cases} (a;b) \in T, \\ (-a,-a) \in T \end{cases} \Rightarrow (a-a, b-a) \in T \Rightarrow (b-a, 0) \in T \Rightarrow (b-a) \in I.$$

Итак, если $b - a = x$, то $(b - a) = x \in I$.

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть T — **конгруенция**. Перейдем это утверждение на язык подмножеств. Пусть F — **отношение**, определенное формулой $F = \{(a,b) \,|\, a + I = b + I\}$. Докажем, что $T \subseteq F$. По **определению конгруенции**, если $(a,b) \in T$, то

$$\begin{cases} (a;b) \in T, \\ (-a,-a) \in T \end{cases} \Rightarrow (a-a, b-a) \in T \Rightarrow (b-a, 0) \in T \Rightarrow (b-a) \in I.$$

Итак, если $b - a = x$, то $(b - a) = x \in I$.
Поэтому $b = a + x$, т.е. $(a,b) \in F$.

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть T — **конгруенция**. Перейдем это утверждение на язык подмножеств. Пусть F — **отношение**, определенное формулой $F = \{(a,b) \,|\, a + I = b + I\}$. Теперь докажем, что $F \subseteq T$.

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть T — **конгруенция**. Перейдем это утверждение на язык подмножеств. Пусть F — **отношение**, определенное формулой $F = \{(a,b) \,|\, a + I = b + I\}$. Теперь докажем, что $F \subseteq T$.

Пусть $(a,b) \in F$. Тогда по **определению конгруенции**

$$\begin{cases} b = a + x, \\ x \in I \end{cases} \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть T — **конгруенция**. Перейдем это утверждение на язык подмножеств. Пусть F — **отношение**, определенное формулой $F = \{(a,b) \,|\, a + I = b + I\}$. Теперь докажем, что $F \subseteq T$.

Пусть $(a,b) \in F$. Тогда по **определению конгруенции**

$$\begin{cases} b = a + x, \\ x \in I \end{cases} \Rightarrow \begin{cases} b = a + x, \\ (x,0) \in T, \\ (-x,-x) \in T \end{cases} \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть T — **конгруенция**. Перейдем это утверждение на язык подмножеств. Пусть F — **отношение**, определенное формулой $F = \{(a,b) \,|\, a + I = b + I\}$. Теперь докажем, что $F \subseteq T$.

Пусть $(a,b) \in F$. Тогда по **определению конгруенции**

$$\begin{cases} b = a + x, \\ x \in I \end{cases} \Rightarrow \begin{cases} b = a + x, \\ (x,0) \in T, \\ (-x,-x) \in T \end{cases} \Rightarrow \begin{cases} b = a + x, \\ (x - x, 0 - x) \in T, \end{cases} \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть T — **конгруенция**. Перейдем это утверждение на язык подмножеств. Пусть F — **отношение**, определенное формулой $F = \{(a,b) \,|\, a + I = b + I\}$. Теперь докажем, что $F \subseteq T$.

Пусть $(a,b) \in F$. Тогда по **определению конгруенции**

$$\begin{cases} b = a + x, \\ x \in I \end{cases} \Rightarrow \begin{cases} b = a + x, \\ (x,0) \in T, \\ (-x,-x) \in T \end{cases} \Rightarrow \begin{cases} b = a + x, \\ (0,-x) \in T, \end{cases} \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть T — **конгруенция**. Перейдем это утверждение на язык подмножеств. Пусть F — **отношение**, определенное формулой $F = \{(a,b) \,|\, a + I = b + I\}$. Теперь докажем, что $F \subseteq T$.

Пусть $(a,b) \in F$. Тогда по **определению конгруенции**

$$\begin{cases} b = a + x, \\ x \in I \end{cases} \Rightarrow \begin{cases} b = a + x, \\ (0,-x) \in T, \end{cases} \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть T — **конгруенция**. Перейдем это утверждение на язык подмножеств. Пусть F — **отношение**, определенное формулой $F = \{(a,b) \,|\, a + I = b + I\}$. Теперь докажем, что $F \subseteq T$.

Пусть $(a,b) \in F$. Тогда по **определению конгруенции**

$$\begin{cases} b = a + x, \\ x \in I \end{cases} \Rightarrow \begin{cases} b = a + x, \\ (0,-x) \in T, \end{cases} \Rightarrow (b + 0, a + x - x) \in T \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть T — **конгруенция**. Перейдем это утверждение на язык подмножеств. Пусть F — **отношение**, определенное формулой $F = \{(a,b) \,|\, a + I = b + I\}$. Теперь докажем, что $F \subseteq T$.

Пусть $(a,b) \in F$. Тогда по **определению конгруенции**

$$\begin{cases} b = a + x, \\ x \in I \end{cases} \Rightarrow \begin{cases} b = a + x, \\ (0,-x) \in T, \end{cases} \Rightarrow (b,a) \in T.$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Осталось доказать, что I — идеал.

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Осталось доказать, что I — идеал.

Докажем, что I — подгруппа аддитивной группы кольца K.

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть $x \in I$ и $y \in I$. По **определению конгруенции** и **теореме об умножении на 0 в кольце с 1**

$$\begin{cases} (x;\ 0) \in T, \\ (y;\ 0) \in T \end{cases} \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть $x \in I$ и $y \in I$. По **определению конгруенции** и **теореме об умножении на 0 в кольце с 1**

$$\begin{cases} (x;\ 0) \in T, \\ (y;\ 0) \in T \end{cases} \Rightarrow (x+y, 0+0) \in T \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть $x \in I$ и $y \in I$. По **определению конгруенции** и **теореме об умножении на 0 в кольце с 1**

$$\begin{cases} (x;\ 0) \in T, \\ (y;\ 0) \in T \end{cases} \Rightarrow\ (x+y, 0+0) \in T\ \Rightarrow\ (x+y, 0) \in T\ \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть $x \in I$ и $y \in I$. По **определению конгруенции** и **теореме об умножении на 0 в кольце с 1**

$$\begin{cases} (x;\ 0) \in T, \\ (y;\ 0) \in T \end{cases} \Rightarrow (x+y, 0+0) \in T \Rightarrow (x+y, 0) \in T \Rightarrow (x+y) \in I.$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть $x \in I$, надо доказать, что $(-x) \in I$. По определению конгруенции

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть $x \in I$, надо доказать, что $(-x) \in I$. По определению конгруенции

$$\begin{cases} (x;\ 0) \in T, \\ (-x;\ -x) \in T \end{cases} \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть $x \in I$, надо доказать, что $(-x) \in I$. По определению конгруенции

$$\begin{cases} (x;\ 0) \in T, \\ (-x;\ -x) \in T \end{cases} \Rightarrow\ (x-x, 0-x) \in T\ \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть $x \in I$, надо доказать, что $(-x) \in I$. По определению конгруенции

$$\begin{cases} (x;\ 0) \in T, \\ (-x;\ -x) \in T \end{cases} \Rightarrow\ (x-x, 0-x) \in T\ \Rightarrow\ (0, -x) \in T\ \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть $x \in I$, надо доказать, что $(-x) \in I$. По определению конгруенции

$$\begin{cases} (x;\ 0) \in T, \\ (-x;\ -x) \in T \end{cases} \Rightarrow\ (x-x, 0-x) \in T\ \Rightarrow\ (0, -x) \in T\ \Rightarrow\ (-x) \in I.$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Осталось показать устойчивость множества I относительно умножения на элементы из K, т.е. что для любого $a \in K$ выполняется $a * I \subseteq I$.

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть $x \in I$ и $a \in K$. По **определению конгруенции** и **теореме об умножении на 0 в кольце с 1**

$$\begin{cases} (x;\ 0) \in T, \\ (a;\ a) \in T \end{cases} \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть $x \in I$ и $a \in K$. По **определению конгруенции** и **теореме об умножении на 0 в кольце с 1**

$$\begin{cases} (x;\ 0) \in T, \\ (a;\ a) \in T \end{cases} \Rightarrow (a * x, a * 0) \in T \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть $x \in I$ и $a \in K$. По **определению конгруенции** и **теореме об умножении на 0 в кольце с 1**

$$\begin{cases} (x;\ 0) \in T, \\ (a;\ a) \in T \end{cases} \Rightarrow (a * x, a * 0) \in T \Rightarrow (a * x, 0) \in T \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть $x \in I$ и $a \in K$. По **определению конгруенции** и **теореме об умножении на 0 в кольце с 1**

$$\begin{cases} (x;\ 0) \in T, \\ (a;\ a) \in T \end{cases} \Rightarrow (a * x, a * 0) \in T \Rightarrow (a * x, 0) \in T \Rightarrow a * x \in I.$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть $x \in I$ и $a \in K$. По **определению конгруенции** и **теореме об умножении на 0 в кольце с 1**

$$\begin{cases} (x;\ 0) \in T, \\ (a;\ a) \in T \end{cases} \Rightarrow (a * x, a * 0) \in T \Rightarrow (a * x, 0) \in T \Rightarrow a * x \in I.$$

Необходимость доказана.

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Докажем достаточность.

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть теперь I — идеал, и отношение T определено правилом: $(a;b) \in T$ тогда и только тогда, когда $a + x = b$ для некоторого x из I. Надо доказать, что T — конгруенция.

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть теперь I — идеал, и отношение T определено правилом: $(a;b) \in T$ тогда и только тогда, когда $a + x = b$ для некоторого x из I. Надо доказать, что T — конгруенция.

Очевидно, что T — отношение эквивалентности.

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть теперь I — идеал, и отношение T определено правилом: $(a;b) \in T$ тогда и только тогда, когда $a + x = b$ для некоторого x из I. Надо доказать, что T — конгруенция.

Очевидно, что T — отношение эквивалентности. Осталось проверить, что

$$\begin{cases} (a;\ b) \in T, \\ (c;\ d) \in T \end{cases} \Rightarrow \begin{cases} (a * c, b * d) \in T, \\ (a + c, b + d) \in T. \end{cases}$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть теперь I — идеал, и отношение T определено правилом: $(a;b) \in T$ тогда и только тогда, когда $a + x = b$ для некоторого x из I. Надо доказать, что T — конгруенция.

$$\begin{cases} (a;\ b) \in T, \\ (c;\ d) \in T \end{cases} \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть теперь I — идеал, и отношение T определено правилом: $(a;b) \in T$ тогда и только тогда, когда $a + x = b$ для некоторого x из I. Надо доказать, что T — конгруенция.

$$\begin{cases} (a;\ b) \in T, \\ (c;\ d) \in T \end{cases} \Rightarrow \begin{cases} (\exists x)\ (x,0) \in T, \\ a + x = b, \\ (\exists y)\ (y,0) \in T, \\ c + y = d. \end{cases} \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть теперь I — идеал, и отношение T определено правилом: $(a;b) \in T$ тогда и только тогда, когда $a + x = b$ для некоторого x из I. Надо доказать, что T — конгруенция.

$$\left\{\begin{array}{l}(a;\ b) \in T,\\ (c;\ d) \in T\end{array}\right. \Rightarrow \left\{\begin{array}{l}(\exists x)\ (x,0) \in T,\\ a + x = b,\\ (\exists y)\ (y,0) \in T,\\ c + y = d.\end{array}\right. \Rightarrow \left\{\begin{array}{l}(\exists x)\ x \in I,\\ (\exists y)\ y \in I,\\ a + x + c + y = b + d,\\ (a + x) * (c + y) = b * d.\end{array}\right. \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть теперь I — идеал, и отношение T определено правилом: $(a;b) \in T$ тогда и только тогда, когда $a + x = b$ для некоторого x из I. Надо доказать, что T — конгруенция.

$$\begin{cases} (a;\ b) \in T, \\ (c;\ d) \in T \end{cases} \Rightarrow \begin{cases} (\exists x)\ x \in I, \\ (\exists y)\ y \in I, \\ a + x + c + y = b + d, \\ (a + x) * (c + y) = b * d. \end{cases} \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть теперь I — идеал, и отношение T определено правилом: $(a;b) \in T$ тогда и только тогда, когда $a + x = b$ для некоторого x из I. Надо доказать, что T — конгруенция.

$$\begin{cases} (a;\ b) \in T, \\ (c;\ d) \in T \end{cases} \Rightarrow \left\{ \begin{array}{l} (\exists x)\ x \in I, \\ (\exists y)\ y \in I, \\ \hline a + x + c + y = b + d, \\ (a + c) + (x + y) = b + d, \\ \hline (a + x) * (c + y) = b * d, \\ a * c + a * y + x * c + x + y = b * d. \end{array} \right. \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть теперь I — идеал, и отношение T определено правилом: $(a;b) \in T$ тогда и только тогда, когда $a + x = b$ для некоторого x из I. Надо доказать, что T — конгруенция.

$$\begin{cases} (a;\ b) \in T, \\ (c;\ d) \in T \end{cases} \Rightarrow \begin{cases} (\exists x)\ x \in I, \\ (\exists y)\ y \in I, \\ (a+c) + \underbrace{(x+y)}_{I} = b + d, \\ a * c + \underbrace{a * y + x * c + x * y}_{I} = b * d. \end{cases} \Rightarrow$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть теперь I — идеал, и отношение T определено правилом: $(a;b) \in T$ тогда и только тогда, когда $a + x = b$ для некоторого x из I. Надо доказать, что T — конгруенция.

$$\begin{cases} (a;\ b) \in T, \\ (c;\ d) \in T \end{cases} \Rightarrow \begin{cases} (a * c, b * d) \in T, \\ (a + c, b + d) \in T. \end{cases}$$

V.1. Теорема о конгруенциях колец

Теорема 12. *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеет место равенство $a + x = b$.*

Доказательство. Пусть теперь I — идеал, и отношение T определено правилом: $(a;b) \in T$ тогда и только тогда, когда $a + x = b$ для некоторого x из I. Надо доказать, что T — конгруенция.

$$\begin{cases} (a;\ b) \in T, \\ (c;\ d) \in T \end{cases} \Rightarrow \begin{cases} (a * c, b * d) \in T, \\ (a + c, b + d) \in T. \end{cases}$$

Следовательно, T — конгруенция, теорема доказана.

V.2. Фактор-кольцо по идеалу

Теорема 12 (о конгруенциях колец). *Отношение T является* ***конгруенцией*** *кольца K тогда и только тогда, когда множество $I = \{x \,|\, (x;0) \in T\}$ является* ***идеалом*** *и $(a;b) \in T$ в том и только том случае, когда для некоторого x из I имеем место равенство $a + x = b$.*

Фактор-кольцо K/T называется **фактор-кольцом** кольца K по идеалу I (идеал I однозначно определяет **конгруенцию** T).

V.3. Теорема о гомоморфизмах полей

Теорема 13 (**о гомоморфизмах полей**). *Всякий* ***гомоморфизм*** *поля* P *в поле* Q *является* ***изоморфизмом***.

Доказательство.

V.3. Теорема о гомоморфизмах полей

Теорема 13 (**о гомоморфизмах полей**). *Всякий* ***гомоморфизм*** *поля* P *в поле* Q *является* ***изоморфизмом***.

Доказательство. Достаточно заметить, что в поле нет отличных от 0 и P идеалов. Применение **теоремы о конгруенциях колец** заканчивает доказательство.

V.4. Теорема об идеалах кольца многочленов

Теорема 14 (**об идеалах кольца многочленов**). *Если* P — ***поле***, *то* ***кольцо*** $P[x]$ *многочленов над полем* P *является* ***кольцом главных идеалов***.

V.4. Теорема об идеалах кольца многочленов

Теорема 14 (об идеалах кольца многочленов). *Если P — **поле**, то **кольцо** $P[x]$ многочленов над полем P является **кольцом главных идеалов**.*

Иными словами, для любого идеала I кольца многочленов $P[x]$ найдется такой многочлен $f(x)$, что многочлен $g(x)$ принадлежит I тогда и только тогда, когда он делится нацело на $f(x)$.

V.4. Теорема об идеалах кольца многочленов

Теорема 14 (об идеалах кольца многочленов). *Если P — **поле**, то **кольцо** $P[x]$ многочленов над полем P является **кольцом главных идеалов**.*

Доказательство. Выберем в I ненулевой многочлен $f(x)$ минимальной степени. Пусть $g(x)$ — произвольный многочлен из I.

V.4. Теорема об идеалах кольца многочленов

Теорема 14 (об идеалах кольца многочленов). *Если P — **поле**, то **кольцо** $P[x]$ многочленов над полем P является **кольцом главных идеалов**.*

Доказательство. Выберем в I ненулевой многочлен $f(x)$ минимальной степени. Пусть $g(x)$ — произвольный многочлен из I.

Разделим $g(x)$ на $f(x)$ с остатком: $g(x) = f(x) * h(x) + r(x)$.

V.4. Теорема об идеалах кольца многочленов

Теорема 14 (об идеалах кольца многочленов). *Если P — **поле**, то **кольцо** $P[x]$ многочленов над полем P является **кольцом главных идеалов**.*

Доказательство. Выберем в I ненулевой многочлен $f(x)$ минимальной степени. Пусть $g(x)$ — произвольный многочлен из I.

Разделим $g(x)$ на $f(x)$ с остатком: $g(x) = f(x) * h(x) + r(x)$. Так как I — **идеал**, то $f(x) * h(x)$ — элемент из I.

V.4. Теорема об идеалах кольца многочленов

Теорема 14 (**об идеалах кольца многочленов**). *Если* P — ***поле***, *то* ***кольцо*** $P[x]$ *многочленов над полем* P *является* ***кольцом главных идеалов***.

Доказательство. Выберем в I ненулевой многочлен $f(x)$ минимальной степени. Пусть $g(x)$ — произвольный многочлен из I.

Разделим $g(x)$ на $f(x)$ с остатком: $g(x) = f(x) * h(x) + r(x)$. Так как I — **идеал**, то $f(x) * h(x)$ — элемент из I.

Следовательно, $r(x) = g(x) + \big(- f(x) * h(x)\big)$ — элемент из I (ведь I — аддитивная подгруппа). Но

V.4. Теорема об идеалах кольца многочленов

Теорема 14 (об идеалах кольца многочленов). *Если P — **поле**, то **кольцо** $P[x]$ многочленов над полем P является **кольцом главных идеалов**.*

Доказательство. Выберем в I ненулевой многочлен $f(x)$ минимальной степени. Пусть $g(x)$ — произвольный многочлен из I.

Разделим $g(x)$ на $f(x)$ с остатком: $g(x) = f(x) * h(x) + r(x)$. Так как I — **идеал**, то $f(x) * h(x)$ — элемент из I.

Следовательно, $r(x) = g(x) + \big(-f(x) * h(x)\big)$ — элемент из I (ведь I — аддитивная подгруппа). Но степень многочлена $r(x)$ меньше степени многочлена $f(x)$, поэтому $r(x) = 0$ (степень многочлена $f(x)$ — минимальная среди всех ненулевых многочленов из I).

V.4. Теорема об идеалах кольца многочленов

Теорема 14 (об идеалах кольца многочленов). *Если* P — ***поле***, *то* ***кольцо*** $P[x]$ *многочленов над полем* P *является* ***кольцом главных идеалов***.

Доказательство. Выберем в I ненулевой многочлен $f(x)$ минимальной степени. Пусть $g(x)$ — произвольный многочлен из I.

Разделим $g(x)$ на $f(x)$ с остатком: $g(x) = f(x) * h(x) + r(x)$. Так как I — **идеал**, то $f(x) * h(x)$ — элемент из I.

Следовательно, $r(x) = g(x) + \big(-f(x) * h(x)\big)$ — элемент из I (ведь I — аддитивная подгруппа). Но степень многочлена $r(x)$ меньше степени многочлена $f(x)$, поэтому $r(x) = 0$ (степень многочлена $f(x)$ — минимальная среди всех ненулевых многочленов из I).

Теорема доказана.

V.5. Теорема о расширении поля как фактор-кольце кольца многочленов

Теорема 15. *Пусть P — поле, $f(x)$ — неприводимый над P многочлен с коэффициентами из P, $I = \left\{ g(x) * f(x) \,\middle|\, g(x) \in P[x] \right\}$ — идеал кольца многочленов, порожденный многочленом $f(x)$, a — корень многочлена $f(x)$ в некотором расширении поля P. Тогда фактор-кольцо $P[x]/I$ изоморфно полю $P[a]$.*

Доказательство.

V.5. Теорема о расширении поля как фактор-кольце кольца многочленов

Теорема 15. *Пусть P — поле, $f(x)$ — неприводимый над P многочлен с коэффициентами из P, $I = \left\{ g(x) * f(x) \,\middle|\, g(x) \in P[x] \right\}$ — идеал кольца многочленов, порожденный многочленом $f(x)$, а — корень многочлена $f(x)$ в некотором расширении поля P. Тогда фактор-кольцо $P[x]/I$ изоморфно полю $P[a]$.*

Доказательство. Рассмотрим отображение F кольца $P[x]$ в поле $P[a]$, определенное формулой:

$$F\left(h(x)\right) = h(a) \in P[a].$$

Легко проверить, что отображение F является **гомоморфизмом**. **Рассмотреть пример?**

V.5. Теорема о расширении поля как фактор-кольце кольца многочленов

Теорема 15. *Пусть P — поле, $f(x)$ — неприводимый над P многочлен с коэффициентами из P, $I = \left\{ g(x) * f(x) \,\middle|\, g(x) \in P[x] \right\}$ — идеал кольца многочленов, порожденный многочленом $f(x)$, a — корень многочлена $f(x)$ в некотором расширении поля P. Тогда фактор-кольцо $P[x]/I$ изоморфно полю $P[a]$.*

Доказательство. $F : P[x] \to P[a]$, где $F\left(h(x)\right) = h(a)$.

Следовательно, по теореме об описании **гомоморфных образов** универсальных алгебр и **теореме о конгруенциях колец** получаем, что $P[a]$ изоморфно $P[x]/J$, где $J = \left\{ h(x) \,\middle|\, F\left(h(x)\right) = 0 \right\} = \{ h(x) \,|\, h(a) = 0 \}$.

V.5. Теорема о расширении поля как фактор-кольце кольца многочленов

Доказательство. $F : P[x] \to P[a]$, где $F\left(h(x)\right) = h(a)$.

Следовательно, по теореме об описании **гомоморфных образов** универсальных алгебр и **теореме о конгруенциях колец** получаем, что $P[a]$ изоморфно $P[x]/J$, где $J = \left\{h(x) \,\middle|\, F\left(h(x)\right) = 0\right\} = \{h(x) \,|\, h(a) = 0\}$.

Осталось доказать, что если $h(a) = 0$, то $h(x)$ делится на $f(x)$.

V.5. Теорема о расширении поля как фактор-кольце кольца многочленов

Доказательство. $F : P[x] \to P[a]$, где $F\left(h(x)\right) = h(a)$.

Следовательно, по теореме об описании **гомоморфных образов** универсальных алгебр и **теореме о конгруенциях колец** получаем, что $P[a]$ изоморфно $P[x]/J$, где $J = \left\{h(x) \middle| F\left(h(x)\right) = 0\right\} = \{h(x) \,|\, h(a) = 0\}$.

По **теореме о делении многочленов с остатком**, получаем, что существуют такие многочлены $u(x)$ и $v(x)$ с коэффициентами из P, что степень многочлена $v(x)$ меньше степени многочлена $f(x)$ и $h(x) = u(x) * f(x) + v(x)$.

V.5. Теорема о расширении поля как фактор-кольце кольца многочленов

Доказательство. $F : P[x] \to P[a]$, где $F\left(h(x)\right) = h(a)$.

Следовательно, по теореме об описании **гомоморфных образов** универсальных алгебр и **теореме о конгруенциях колец** получаем, что $P[a]$ изоморфно $P[x]/J$, где $J = \left\{h(x) \middle| F\left(h(x)\right) = 0\right\} = \{h(x) \,|\, h(a) = 0\}$.

По **теореме о делении многочленов с остатком**, получаем, что существуют такие многочлены $u(x)$ и $v(x)$ с коэффициентами из P, что степень многочлена $v(x)$ меньше степени многочлена $f(x)$ и $h(x) = u(x) * f(x) + v(x)$. Остается заметить, что

$$0 = h(a) = u(a) * f(a) + v(a) = u(a) * 0 + v(a) = v(a).$$

V.5. Теорема о расширении поля как фактор-кольце кольца многочленов

Доказательство. $F : P[x] \to P[a]$, где $F\left(h(x)\right) = h(a)$.

Следовательно, по теореме об описании **гомоморфных образов** универсальных алгебр и **теореме о конгруенциях колец** получаем, что $P[a]$ изоморфно $P[x]/J$, где $J = \left\{h(x) \,\middle|\, F\left(h(x)\right) = 0\right\} = \{h(x) \,|\, h(a) = 0\}$.

Итак, степень многочлена $v(x)$ меньше степени многочлена $f(x)$, $h(x) = u(x) * f(x) + v(x)$ и $v(a) = 0$. Но $f(x)$ — ненулевой многочлен минимальной степени такой, что $f(a) = 0$. Значит $v(x)$ — нулевой многочлен.

V.5. Теорема о расширении поля как фактор-кольце кольца многочленов

Доказательство. $F : P[x] \to P[a]$, где $F\left(h(x)\right) = h(a)$.

Следовательно, по теореме об описании **гомоморфных образов** универсальных алгебр и **теореме о конгруенциях колец** получаем, что $P[a]$ изоморфно $P[x]/J$, где $J = \left\{h(x) \,\middle|\, F\left(h(x)\right) = 0\right\} = \{h(x) \,|\, h(a) = 0\}$.

Итак, степень многочлена $v(x)$ меньше степени многочлена $f(x)$, $h(x) = u(x) * f(x) + v(x)$ и $v(a) = 0$. Но $f(x)$ — ненулевой многочлен минимальной степени такой, что $f(a) = 0$. Значит $v(x)$ — нулевой многочлен.

Следовательно, $J = I$.

V.5. Теорема о расширении поля как фактор-кольце кольца многочленов

Теорема 15. *Пусть P — поле, $f(x)$ — неприводимый над P многочлен с коэффициентами из P, $I = \left\{ g(x) * f(x) \,\middle|\, g(x) \in P[x] \right\}$ — идеал кольца многочленов, порожденный многочленом $f(x)$, a — корень многочлена $f(x)$ в некотором расширении поля P. Тогда фактор-кольцо $P[x]/I$ изоморфно полю $P[a]$.*

Доказательство. $F : P[x] \to P[a]$, где $F\left(h(x)\right) = h(a)$.

По теореме об описании **гомоморфных образов** универсальных алгебр и **теореме о конгруенциях колец** получаем, что $P[a]$ изоморфно $P[x]/J$, где $J = \left\{ h(x) \,\middle|\, F\left(h(x)\right) = 0 \right\} = \left\{ h(x) \,\middle|\, h(a) = 0 \right\}$, причем мы доказали, что $J = I$.

V.5. Теорема о расширении поля как фактор-кольце кольца многочленов

Теорема 15. *Пусть P — поле, $f(x)$ — неприводимый над P многочлен с коэффициентами из P, $I = \left\{ g(x) * f(x) \,\middle|\, g(x) \in P[x] \right\}$ — идеал кольца многочленов, порожденный многочленом $f(x)$, a — корень многочлена $f(x)$ в некотором расширении поля P. Тогда фактор-кольцо $P[x]/I$ изоморфно полю $P[a]$.*

Теорема доказана.

Спасибо за внимание!

e-mail: melnikov@k66.ru, melnikov@r66.ru
сайты: http://melnikov.k66.ru, http://melnikov.web.ur.ru

Вернуться к списку презентаций?