

Министерство науки и высшего образования Российской Федерации  
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ  
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Радиофизический факультет

УТВЕРЖДЕНО:

Декан

А. Г. Коротаев

Оценочные материалы по дисциплине

Общая алгебра

по направлению подготовки

**03.03.03 Радиофизика**

Направленность (профиль) подготовки:

**Радиофизика, электроника и информационные системы**

Форма обучения

**Очная**

Квалификация

**Бакалавр**

Год приема

**2025**

СОГЛАСОВАНО:

Руководитель ОП

М.Л. Громов

Председатель УМК

А.П. Коханенко

Томск – 2025

## 1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-1 Способен применять базовые знания в области физики и радиофизики и использовать их в профессиональной деятельности, в том числе в сфере педагогической деятельности;

ПК-1 Способен проанализировать поставленную задачу в области радиофизики и электроники, осуществлять поиск, обобщение и использование научно-технической информации, необходимой для эффективного выполнения профессиональной задачи..

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК 1.3 Применяет базовые знания в области физики и радиофизики при осуществлении профессиональной деятельности.

ИПК 1.1 Понимает требования, предъявляемые к исследуемому прибору, устройству или системе и ожидаемые результаты их использования.

ИПК 1.2 Эффективно осуществляет поиск теоретических и экспериментальных данных в исследуемой и смежных областях деятельности, необходимых для решения поставленной задачи.

ИПК 1.3 Производит сравнительный анализ вариантов решения задачи, определение рисков, связанных с реализацией различных вариантов.

## 2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля в пятом семестре:

- тесты;
- контрольная работа.

Тест 1 (ИОПК 1.3, ИПК 1.1, ИПК 1.2)

Примеры вопросов:

1. Пусть  $A = \{1, 2, 3, 4\}$ . Тогда булеан  $2^A$  содержит

- а) 8 элементов
- б) 3 элемента
- в) 15 элементов
- г) 4 элемента
- д) 7 элементов
- е) 16 элементов

2. Заданы множества  $A = \{a, b, c\}$  и  $B = \{a, b, e\}$ .

Тогда декартово произведение  $A \times B$  содержит пары:

- а) (a, a), (a, b), (e, a), (b, a), (b, b), (b, e), (c, a), (c, b), (c, e)
- б) (a, a), (a, b), (a, e), (b, a), (b, b), (b, e), (c, a), (c, b), (c, e)
- в) (a, a), (a, b), (a, e), (b, a), (b, b), (b, e), (c, a), (c, b), (e, c)
- г) (a, a), (b, a), (e, a), (a, b), (b, b), (e, b), (a, c), (b, c), (e, c)
- д) (a, a), (a, b), (a, e), (b, a), (b, b), (e, b), (c, a), (c, b), (c, e)

3. Пусть отношения  $\varphi_1 \subseteq A \times B$ ,  $\varphi_2 \subseteq B \times C$ , где  $A = \{4, 7, 5\}$ ,  $B = \{2, 3, 8\}$  и  $C = \{10, 11\}$ . Какие пары могут принадлежать композиции  $\varphi_1 \circ \varphi_2$ ?

- а) (4, 2)
- б) (7, 10)
- в) (8, 11)
- г) (5, 8)
- д) (2, 8)

4. Какими свойствами обладает отношение "равенства" на множестве треугольников?

- а) Антисимметричность
- б) Интразитивность
- в) Симметричность
- г) Нереклексивность
- д) Нетранзитивность
- е) Несимметричность
- ж) Транзитивность
- з) Релексивность
- и) Антирелексивность

5. Какими свойствами обладает отношение "быть делителем" на множестве натуральных чисел?

- а) Антисимметричность
- б) Интразитивность
- в) Симметричность
- г) Нереклексивность
- д) Нетранзитивность
- е) Несимметричность
- ж) Транзитивность
- з) Релексивность
- и) Антирелексивность

Ключи: 1 е), 2 б), 3 б), 4 в)ж)з), 5 а)ж)з).

Тест считается пройденным, если обучающийся ответил правильно как минимум на 70% вопросов.

Контрольная работа 1 (ИПК 1.1, ИПК 1.2, ИПК 1.3)

Контрольная работа состоит из 7 задач.

Примеры задач:

1. Вычислить НОД(1173, 323) с помощью алгоритма Евклида.

2. Найти показатель, с которым число 5 входит в 643!

3. Вычислить  $2^{199} \bmod 1003$ .

4. Найти наименьшее положительное  $x$ , удовлетворяющее системе уравнений:

$$x \equiv 2 \pmod{3}$$

$$x \equiv 4 \pmod{11}$$

$$x \equiv 5 \pmod{7}$$

5. Найти остаток от деления  $171^{2405}$  на 52.

6. Найти  $b = 6^{-1} \bmod 15$

7. Определить, является ли 7411 квадратичным вычетом по модулю простого числа 9283.

Ответы:

Задача 1. 17.

Задача 2. 159.

Задача 3. 247.

Задача 4. 26.

Задача 5. 19.

Задача 6. 2.

Задача 7. Нет.

Критерии оценивания:

Результаты контрольной работы определяются оценками «зачтено», «не зачтено».

Оценка «зачтено» выставляется, если решены все задачи, возможно с небольшими неточностями.

Оценка «не зачтено» выставляется, если задачи не решены или решены с грубыми ошибками.

Элементы текущего контроля по дисциплине в шестом семестре:

- тесты;
- контрольные работы.

Тест 2 (ИОПК 1.3, ИПК 1.1, ИПК 1.2)

Примеры вопросов:

1. Множество  $A$  с введенной на нём операцией  $*$  называется полугруппой, если:

- а) операция  $*$  дистрибутивна
- б) операция  $*$  идемпотентна
- в) операция  $*$  ассоциативна
- г) операция  $*$  рефлексивна
- д) операция  $*$  транзитивна
- е) операция  $*$  коммутативна
- ж) нет верного ответа

2. Множество  $A$  с введенной на нём операцией  $*$  является группой, если выполняются следующие условия...

- а) В  $A$  существует единичный элемент
- б) Если операция  $*$  является сложением или умножением
- в) Если  $A$  не является полугруппой
- г) Для каждого элемента из множества  $A$  найдется обратный элемент из этого же множества

- д) Операция  $*$  ассоциативна
- е) Нет верного ответа
- ж) Операция  $*$  дистрибутивна
- з) В  $A$  нет нулевого элемента

3. На множестве  $A$  задана операция  $+$ , на множестве  $B$  задана операция  $*$ .

Отображение  $\varphi: A \rightarrow B$  называется гомоморфизмом, если ...

- а)  $\forall x, y \in A \quad \varphi(x + y) = \varphi(x * y)$
- б)  $\forall x, y \in A \quad \varphi(x + y) = \varphi(x) * \varphi(y)$
- в)  $\forall x, y \in A \quad \varphi(x) + \varphi(y) = \varphi(x) * \varphi(y)$
- г)  $\forall x, y \in A \quad \varphi(x) + \varphi(y) = \varphi(x * y)$
- д) нет верного ответа

Ключи: 1 в), 2 а)г)д), 3 б).

Тест считается пройденным, если обучающийся ответил правильно как минимум на 70% вопросов.

Контрольная работа 2 (ИПК 1.1, ИПК 1.2, ИПК 1.3)

Контрольная работа состоит из 3 задач.

Примеры задач:

1. Образуют ли полугруппу/группу

- 1) вещественные числа относительно вычитания;
- 2) вещественные числа относительно операции  $-a - b$ ;
- 3) вещественные числа кроме нуля относительно деления;
- 4) натуральные числа относительно операции НОД  $\{a, b\}$ ?

2. Доказать, что множество всех отображений множества  $\{1, 2, \dots, n\}$  в себя относительно операции композиции (произведения) образует полугруппу, но (при  $n > 1$ ) не группу.

3. Образует ли полугруппу/группу множество положительных вещественных чисел относительно указанной операции:

- 1)  $a \circ b = ab$ ;
- 2)  $a \circ b = a^2 b^2$ ?

Ответы:

Задача 1. 1) полугруппой не является; 2) полугруппой не является; 3) полугруппой не является; 4) полугруппа с единицей, но не группа.

Задача 3. 1) полугруппой не является, 2) полугруппой не является.

Критерии оценивания:

Результаты контрольной работы определяются оценками «зачтено», «не зачтено».

Оценка «зачтено» выставляется, если решены все задачи, возможно с небольшими неточностями.

Оценка «не зачтено» выставляется, если задачи не решены или решены с грубыми ошибками.

Контрольная работа 3 (ИПК 1.1, ИПК 1.2, ИПК 1.3).

Контрольная работа состоит из 3 задач.

Примеры задач:

1. Является ли кольцом/полем

алгебраическая система  $\langle B, \vee, \& \rangle$  ;

алгебраическая система  $\langle B, \oplus, \& \rangle$  ?

2. Решить систему линейных уравнений в поле  $Z_3$ :

$$x + 2y + 2z = 1;$$

$$2x + y + 2z = 2;$$

$$2x + 2y + z = 2.$$

3. Найти НОД многочленов  $x^5 - x^4 - 2x^3 + 2x^2 + 9x - 9$  и  $x^5 + x^4 + 4x^3 - x^2 + x - 6$  над полем  $Z_5$ .

Ответы:

Задача 1. 1) Не является кольцом; 2) является полем.

Задача 2.  $x = 1, y = 0, z = 0$ .

Задача 3.  $x^3 + x + 3$ .

Критерии оценивания:

Результаты контрольной работы определяются оценками «зачтено», «не зачтено».

Оценка «зачтено» выставляется, если решены все задачи, возможно с небольшими неточностями.

Оценка «не зачтено» выставляется, если задачи не решены или решены с грубыми ошибками.

### **3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания**

Промежуточная аттестация (зачет) по дисциплине в пятом семестре проводится в письменной форме. К промежуточной аттестации допускаются только те студенты, которые успешно прошли текущие аттестации по практическим занятиям. Продолжительность зачета 1 час.

Каждый билет для промежуточной аттестации состоит из двух частей по темам из разных разделов дисциплины. В качестве дополнительных вопросов во время проведения промежуточной аттестации используются контрольные вопросы, предлагаемые для самостоятельной работы обучающегося.

Первая часть содержит два вопроса, проверяющие ИОПК 1.3, ИПК 1.1, ИПК 1.2. Ответы на вопросы первой части даются в развернутой форме.

Вторая часть содержит 2 вопроса, проверяющих ИПК 1.1, ИПК 1.3, и оформленные в виде практических задач. Ответы на вопросы второй части предполагают решение задач и краткую интерпретацию полученных результатов.

Перечень теоретических вопросов:

Отношения.

1. Множества, основные операции над множествами, декартово произведение множеств.

2. Отношение на паре множеств, бинарное отношение на множестве, примеры отношений.

3. Основные операции над отношениями (произведение отношений, построение обратного отношения).

4. Свойства бинарных отношений (с примерами: один пример на каждое свойство).

5. Отношение эквивалентности (с примерами: 2 примера эквивалентностей).

6. Доказать, что по каждому разбиению множества можно задать эквивалентность на этом множестве.

7. Доказать, что каждая эквивалентность на множестве отвечает некоторому разбиению этого множества.

8. Привести примеры эквивалентностей на множестве и разбиений, которым они отвечают.

9. Отношение порядка, максимальный (минимальный) и наибольший (наименьший) элементы частично упорядоченного множества (с примером).

10. Верхняя и нижняя полурешетки (с примером).

11. Является ли множество всех подмножеств некоторого множества решеткой относительно отношения включения? (Ответ обосновать)

12. Отношение линейного порядка (с примерами: 2 примера линейно упорядоченных множеств).

13. Отображения: в, на, взаимно однозначное отображение (с примерами: один пример на каждое отображение).

14. Подстановки, утверждение о числе различных подстановок на множестве  $\{1, 2, \dots, n\}$  (с доказательством).

15. Бинарная операция на множестве, 2 примера множеств с заданными операциями.

Теория чисел.

1. Общие делители, наибольший общий делитель.

2. Общие кратные, наименьшее общее кратное.

3. Простые и составные числа. Взаимно простые числа, попарно простые числа.

4. Теорема о наименьшем делителе целого числа.

5. Каноническое представление целого числа.

6. Непрерывные дроби. Закон образования подходящих дробей.

7. Свойства мультипликативных функций.

8. Теоремы о сумме и числе делителей натурального числа.

9. Функция Эйлера, формулы ее вычисления.

10. Свойства сравнений.

11. Полная и приведенная системы вычетов.

12. Теоремы Эйлера и Ферма. Обобщенная теорема Эйлера.

13. Понижение степени сравнения.
14. Способы нахождения решений сравнений первой степени с одним неизвестным.
15. Китайская теорема об остатках.
16. Теорема Вильсона.
17. Критерии Эйлера и Гаусса.
18. Символ Лежандра, его свойства.
19. Порядок числа по заданному модулю.
20. Первообразные корни.

Примеры задач:

1. Найдите НОД (739; 1 999).
2. Верно ли числовое сравнение:  $39 \equiv 15 \pmod{14}$ ?
3. Установите, сравнимы ли числа 841 и 284 по модулю 7, пользуясь а) определением; б) признаком сравнимости чисел по модулю
4. Найдите остаток от деления  $79^2 + 21^3$  на 13.
5. Найти обратный элемент  $b = 160^{-1}$  по  $\text{mod } 841$ .
6. Используя свойства символа Лежандра, определите, сколько решений имеет сравнение:  $x^2 \equiv 26 \pmod{71}$ .
7. Среди вычетов приведенной системы по модулю 19 укажите квадратичные вычеты.

Результаты зачета определяются оценками «Зачтено», «Не зачтено».

Оценка «Зачтено» выставляется, если на все теоретические вопросы даны развернутые ответы и все задачи решены без ошибок или с небольшими ошибками.

Оценка «Не зачтено» выставляется, если хотя бы на один из теоретических вопросов не дано ответа и/или хотя бы одна из задач не решена или решена с грубыми ошибками.

Промежуточная аттестация по дисциплине в шестом семестре проводится в форме письменного экзамена. К промежуточной аттестации допускаются только те студенты, которые успешно прошли текущие аттестации по практическим занятиям.

Каждый билет для промежуточной аттестации состоит из двух частей по темам из разных разделов дисциплины. В качестве дополнительных вопросов во время проведения промежуточной аттестации используются контрольные вопросы, предлагаемые для самостоятельной работы обучающегося. Продолжительность экзамена 1,5 часа.

Первая часть содержит два вопроса, проверяющие ИОПК 1.3, ИПК 1.1, ИПК 1.2. Ответы на вопросы первой части даются в развернутой форме.

Вторая часть содержит 2 вопроса, проверяющих ИПК 1.1, ИПК 1.3, и оформленные в виде практических задач. Ответы на вопросы второй части предполагают решение задач и краткую интерпретацию полученных результатов.

Перечень теоретических вопросов:

Группы.

1. Понятие полугруппы; 3 примера полугрупп.
2. Понятие группы; пример группы; теоремы единственности единичного и обратного элементов в группе (с доказательством).
3. Понятие подгруппы группы; критерий «быть подгруппой» (с доказательством); теорема о пересечении конечного числа подгрупп группы (с доказательством).
4. Разложение группы по подгруппе; критерий принадлежности двух элементов группы одному левому смежному классу по подгруппе (с доказательством).
5. Разложение группы по подгруппе; теорема о разбиении множества элементов группы на левые смежные классы (с доказательством).

6. Индекс подгруппы в группе; теорема Лагранжа (с доказательством).
7. Нормальная подгруппа; критерий проверки «нормальности» подгруппы (через сопряженные подгруппы) (с доказательством).
8. Фактор-группы; теорема о том, что фактор-группа, образует группу относительно операции умножения смежных классов (с доказательством).
9. Циклические группы; порядок элемента; теорема о подгруппе циклической группы (с доказательством).
10. Гомоморфизмы групп; теорема о гомоморфном образе группы (с доказательством).
11. Гомоморфизмы групп; теорема о гомоморфизмах групп (в двух положениях) (с доказательством).
12. Прямое произведение групп. Критерий разложимости группы в прямое произведение своих подгрупп (с доказательством).
13. Нормальные и композиционные ряды в группах.  
Кольца и поля.
  1. Определение кольца; теорема об основных соотношениях в кольце.
  2. Кольцо многочленов.
  3. Определение поля; 2 примера поля.
  4. Кольцо классов вычетов по идеалу.
  5. Понятие делимости и алгоритм деления Евклида для целых чисел.
  6. Кольцо классов вычетов целых чисел; доказать, что совокупность целых чисел образует идеал тогда и только тогда, когда она состоит из всех чисел, кратных некоторому целому числу.
  7. Кольцо классов вычетов целых чисел.
  8. Кольцо классов вычетов целых чисел. Простые поля Галуа.
  9. Многочлены над полем: нормированный многочлен, неприводимый многочлен, теорема деления для многочленов, алгоритм деления Евклида для многочленов.
  10. Теорема Безу (с доказательством).
  11. Идеал в кольце многочленов; сформулировать три теоремы для кольца многочленов, аналогичные теоремам для идеала в кольце целых чисел. Определения расширения и характеристики поля Галуа.
  12. Доказать, что в поле характеристики  $p$  имеет место равенство  $(a + b)^p = a^p + b^p$ .
  13. Минимальная функция; 2 теоремы о свойствах минимальной функции (с доказательством).
  14. Определение системы линейных уравнений над полем; совместные и несовместные системы; однородные и неоднородные системы.
  15. Примитивный элемент в поле Галуа. Дискретное логарифмирование в полях Галуа.
  16. Метод решения однородной системы линейных уравнений над полем.  
Примеры задач:
    1. Образуют ли полугруппу/группу вещественные числа относительно вычитания?
    2. Построить разложение группы  $G = (B_3, \oplus)$  на левые смежные классы по подгруппе  $H$ , состоящей из булевых векторов длины 3, у которых вторая компонента равна нулю.
    3. Доказать, что если объединение двух подгрупп  $H$  и  $K$  группы  $G$  является подгруппой, то либо  $H$  подгруппа в  $K$ , либо  $K$  подгруппа в  $H$ .
    4. Для аддитивной группы целых чисел  $(Z, +)$  построить фактор-группу  $Z/Z_3$ .
    5. Показать, что подгруппа, индекс которой есть наименьший простой делитель порядка группы, нормальна.
    6. Является ли полем  $(B, \vee, \&)$ ?
    7. Показать, что  $(\{0, 1, \dots, p-1\}, + \bmod p, * \bmod p)$  – кольцо.

Результаты экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» выставляется, если на все теоретические вопросы даны развернутые ответы и задачи решены без ошибок.

Оценка «хорошо» выставляется, если на все теоретические вопросы даны развернутые ответы и задачи решены с небольшими ошибками.

Оценка «удовлетворительно» выставляется, если на один теоретический вопрос не дан развернутый ответ и задачи решены с небольшими ошибками.

Оценка «неудовлетворительно» выставляется, если на один или два теоретических вопроса не дан развернутый ответ и/или задачи не решены или решены с грубыми ошибками.

#### **4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)**

Тест (ИОПК 1.3, ИПК 1.1, ИПК 1.2, ИПК 1.3)

1. Какие пары принадлежат декартову произведению  $A \times B$ , где  $A = \{2, 5, 7, 10\}$  и  $B = \{41, 77, 79\}$ ?

- а) (5, 79)
- б) (10, 79)
- в) (5, 7)
- г) (41, 2)
- д) (77, 7)

2. Что такое отношение?

а) Всякое подмножество объединения множеств  $A$  и  $B$  называется отношением, определенным на паре множеств  $A$  и  $B$

б) Всякое подмножество пересечения множеств  $A$  и  $B$  называется отношением, определенным на паре множеств  $A$  и  $B$

в) Всякое подмножество декартова произведения  $A$  на  $B$  называется отношением, определенным на паре множеств  $A$  и  $B$

3. Выберите операции на отношениях

- а) Произведение отношений
- б) Разность отношений
- в) Пересечение отношений
- г) Объединение отношений
- д) Обратное отношение

4. Какими свойствами обладает отношение эквивалентности?

- а) Симметричность
- б) Антисимметричность
- в) Транзитивность
- г) Рефлексивность

5. Отношение порядка (частичного порядка) обладает свойствами

- а) Транзитивность
- б) Симметричность
- в) Рефлексивность
- г) Антисимметричность

6. Разбиение множества - это ...

а) это представление его в виде пересечения произвольного количества попарно непересекающихся непустых подмножеств

б) это представление его в виде объединения произвольного количества попарно пересекающихся непустых подмножеств

в) это представление его в виде объединения произвольного количества попарно непересекающихся непустых подмножеств

7. Покрытие множества - это ...

- а) семейство множеств, таких, что их разность содержит заданное множество
- б) семейство множеств, таких, что их объединение содержит заданное множество
- в) семейство множеств, таких, что их пересечение содержит заданное множество

8. Множество называется решеткой, если ...

- а) любая пара его элементов имеет и верхние, и нижние границы
- б) любая пара его элементов сравнима
- в) любая пара его элементов имеет и верхнюю, и нижнюю грань

9. Выберите верные утверждения

а) Биективное отображение множества  $\{1, 2, \dots, n\}$  на себя называется подстановкой на этом множестве

б) Отображение  $f: A \rightarrow B$  называется сюръективным, если у каждого элемента  $b \in B$  есть, по крайней мере, один прообраз

в) Отображение нельзя определять на декартовом произведении множеств

г) Сюръективное отображение называется биективным, если обратное ему отображение является сюръективным

10. Множество  $A$  с введенной на нём операцией  $*$  называется полугруппой, если:

- а) операция  $*$  транзитивна
- б) операция  $*$  ассоциативна
- в) операция  $*$  рефлексивна
- г) нет верного ответа
- д) операция  $*$  дистрибутивна
- е) операция  $*$  идемпотентна
- ж) операция  $*$  коммутативна

11. Выберите полугруппы.

- а) Множество натуральных чисел относительно умножения
- б) Множество четных чисел относительно умножения
- в) Множество вещественных чисел относительно деления
- г) Множество четных чисел относительно вычитания
- д) Множество целых чисел относительно вычитания
- е) Множество целых чисел относительно деления
- ж) Множество натуральных чисел относительно сложения
- з) Множество целых неположительных чисел относительно сложения

12. Множество  $A$  с введенной на нем операцией  $*$  является группой, если выполняются следующие условия...

- а) В  $A$  существует единичный элемент
- б) Если операция  $*$  является сложением или умножением
- в) Если  $A$  не является полугруппой
- г) Для каждого элемента из множества  $A$  найдется обратный элемент из этого же множества

- д) Операция  $*$  ассоциативна
- е) Нет верного ответа
- ж) Операция  $*$  дистрибутивна
- з) В  $A$  нет нулевого элемента

13. На множестве  $G = \{a, b, c, d, e\}$  введена операция умножения согласно таблице:

	<b>a</b>	<b>b</b>	<b>c</b>	<b>d</b>	<b>e</b>
<b>a</b>	<i>d</i>	<i>e</i>	<i>b</i>	<i>a</i>	<i>c</i>
<b>b</b>	<i>c</i>	<i>d</i>	<i>e</i>	<i>b</i>	<i>a</i>
<b>c</b>	<i>e</i>	<i>a</i>	<i>d</i>	<i>c</i>	<i>b</i>
<b>d</b>	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>
<b>e</b>	<i>b</i>	<i>c</i>	<i>a</i>	<i>e</i>	<i>d</i>

Является ли  $G$  группой? Если да, укажите элемент, обратный для  $b$ .

- а)  $e$
- б)  $b$
- в)  $d$
- г)  $c$
- д)  $a$
- е)  $G$  не является группой

14. Задана группа  $G$  с групповой операцией  $*$ .  $H$  является подмножеством элементов группы  $G$ .  $H$  - подгруппа группы  $G$ , если и только если...

- а)  $\forall x, y \in H \quad x*y \in H$
- б)  $\forall x \in H \quad x^{-1} \in G$
- в)  $\forall x, y \in G \quad x*y \in H$
- г)  $\forall x \in H \quad x^{-1} \in H$
- д)  $\forall x, y \in H \quad x*y \in G$
- е)  $|H| \geq |G|$
- ж)  $\forall x \in G \quad x^{-1} \in H$
- з)  $|H| \leq |G|$

15. Пусть  $G$  - группа с операцией  $*$  и  $H$  - её нормальная подгруппа. Выберите верные утверждения.

- а)  $\forall a \in G \quad aH = Ha$
- б)  $\forall a \in G$  и  $\forall h \in H \quad a * h = h * a$
- в) Операция  $*$  ассоциативна
- г) Операция  $*$  коммутативна
- д)  $\forall a \in G$  и  $\forall h \in H \quad \exists$  единственный  $h' \in H$  такой, что  $a * h = h' * a$

16. На множестве  $A$  задана операция  $+$ , на множестве  $B$  задана операция  $*$ . Отображение  $\varphi: A \rightarrow B$  называется гомоморфизмом, если ...

- а)  $\forall x, y \in A \quad \varphi(x + y) = \varphi(x) * \varphi(y)$
- б)  $\forall x, y \in A \quad \varphi(x) + \varphi(y) = \varphi(x * y)$
- в)  $\forall x, y \in A \quad \varphi(x) + \varphi(y) = \varphi(x) * \varphi(y)$
- г)  $\forall x, y \in A \quad \varphi(x + y) = \varphi(x * y)$
- д) нет верного ответа

17. На множестве  $A$  заданы операции  $+$  и  $*$ .  $(A, +, *)$  является кольцом, если...

- а)  $\forall x, y, z \in A \quad (y + z) * x = y * x + z * x$
- б)  $(A, +)$  - группа
- в)  $\forall x, y, z \in A \quad x * (y + z) = x * y + x * z$
- г)  $(A, *)$  - полугруппа
- д)  $(A \setminus \{0\}, *)$  - абелева группа
- е) Операция  $+$  коммутативна

18. На множестве  $A$  заданы операции  $+$  и  $*$ .  $(A, +, *)$  является полем, если...

- а)  $(A, +)$  - группа
- б)  $\forall x, y, z \in A \quad (y + z) * x = y * x + z * x$
- в) Операция  $+$  коммутативна
- г)  $(A \setminus \{0\}, *)$  - абелева группа
- д)  $\forall x, y, z \in A \quad x * (y + z) = x * y + x * z$
- е)  $(A, *)$  - полугруппа

19. Решить уравнение в поле Галуа из 11 элементов.

$$x^2 = 5$$

$$x = \dots\dots$$

а) 0

б) 9

в) 4

г) 7

д) 5

е) 10

20. В поле характеристики 2 верно:

а)  $(a+b)^2 = a^2 + 2ab + b^2$

б)  $(a+b)^2 = a^2 + b^2$

в)  $(a+b)^2 = a^2 - b^2$

г)  $(a-b)^2 = a^2 - 2ab + b^2$

21. Вычислить  $2^{199} \bmod 1003$

а) 247

б) 305

в) 34

г) 19

22. Найти наименьшее положительное  $x$ , удовлетворяющее системе уравнений:

$$x \equiv 2 \pmod{3}$$

$$x \equiv 4 \pmod{11}$$

$$x \equiv 5 \pmod{7}$$

а) 19

б) 26

в) 23

г) 18

23. Найти остаток от деления  $171^{2405}$  на 52.

а) 30

б) 27

в) 19

г) 18

Ключи: 1 а)б), 2 в), 3 а)з), 4 а)в)г), 5 а)в)г), 6 в), 7 б), 8 в), 9 а)б)г), 10 б), 11 а)б)ж)з), 12 а)г)д), 13 б), 14 а)г), 15 а)в)д), 16 а), 17 а)б)в)г)е), 18 а)б)г)д), 19 в)г), 20 б), 21 а), 22 б), 23 в).

Теоретические вопросы:

1. Множества, основные операции над множествами, декартово произведение множеств. (ИОПК 1.3, ИПК 1.2)

Ответ должен содержать описание основных операций над множествами (пересечение, объединение, разность, симметрическая разность, дополнение, декартово произведение множеств).

2. Отношение на паре множеств. Основные операции над отношениями. Свойства бинарных отношений. (ИОПК 1.3, ИПК 1.2)

Ответ должен содержать описание понятий отношения на паре множеств, бинарного отношения, основных операций над отношениями (произведение, обратное отношение). Также ответ должен содержать описание свойств бинарных отношений (симметричность, рефлексивность, транзитивность, антисимметричность).

3. Отношение эквивалентности. Отношение порядка. Отношение линейного порядка. (ИОПК 1.3, ИПК 1.2)

Ответ должен содержать описание понятий отношений эквивалентности, порядка и линейного порядка. Должны быть перечислены свойства данных отношений.

4. Отображения:  $v$ ,  $na$ , взаимно однозначное отображение. (ИОПК 1.3, ИПК 1.2)

Ответ должен содержать описание понятия отображения, а также различных видов отображений ( $v$ ,  $na$ , взаимно однозначное отображение).

5. Понятие делимости для целых чисел. Расширенный алгоритм Евклида. Классы вычетов целых чисел. (ИОПК 1.3, ИПК 1.2)

Ответ должен содержать описание понятия делимости для целых чисел, классов вычетов целых чисел. Также ответ должен содержать описание алгоритма Евклида для поиска наибольшего общего делителя.

6. Понятие сравнимости целых чисел. Полная и приведенная система вычетов. (ИОПК 1.3, ИПК 1.2)

Ответ должен содержать описание основных понятий модулярной арифметики, сравнимости целых чисел, свойства сравнений, полной и приведенной системы вычетов.

7. Полугруппа, группа, подгруппа. (ИОПК 1.3, ИПК 1.2)

Ответ должен содержать описание понятий полугруппы, группы, подгруппы, абелевой группы, алгоритм разложения группы по подгруппе.

8. Нормальная подгруппа. Фактор-группа. (ИОПК 1.3, ИПК 1.2)

Ответ должен содержать критерий «нормальности» подгруппы, понятие фактор-группы.

9. Гомоморфизмы групп. (ИОПК 1.3, ИПК 1.2)

Ответ должен содержать описание понятия гомоморфизма групп, изоморфизма групп, теорему о гомоморфизмах групп.

10. Кольцо. Идеалы в кольце. Кольцо классов вычетов. (ИОПК 1.3, ИПК 1.2)

Ответ должен содержать определение кольца, его свойства, определение идеала в кольце. Также ответ должен содержать определение кольца классов вычетов.

11. Поле. Поле Галуа. Свойства полей Галуа. Решение систем уравнений в полях Галуа. (ИОПК 1.3, ИПК 1.2)

Ответ должен содержать определение поля, поля Галуа и его свойства, в том числе свойства минимальной функции. Также ответ должен содержать описание процесса решения систем уравнений в полях Галуа.

### **Информация о разработчиках**

Широкова Екатерина Владимировна, радиофизический факультет, кафедра информационных технологий в исследовании дискретных структур, старший преподаватель.