

**Федеральное государственное автономное образовательное
учреждение высшего образования
«Московский физико-технический институт
(национальный исследовательский университет)»**

УТВЕРЖДЕНО

**Директор физтех-школы
прикладной математики и
информатики**

А.М. Райгородский

	Рабочая программа дисциплины (модуля)
по дисциплине:	Теория колец и полей
по направлению:	Прикладная математика и информатика
профиль подготовки:	Математика Физтех-школа Прикладной Математики и Информатики кафедра дискретной математики
курс:	2
квалификация:	бакалавр

Семестр, формы промежуточной аттестации: 4 (весенний) - Экзамен

Аудиторных часов: 60 всего, в том числе:

лекции: 30 час.

семинары: 30 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 45 час.

Подготовка к экзамену: 30 час.

Всего часов: 135, всего зач. ед.: 3

Количество контрольных работ, заданий: 2

Программу составил: Д.Г. Ильинский, канд. экон. наук, доцент

Программа обсуждена на заседании кафедры дискретной математики 05.03.2020

Аннотация

Курс «Теория колец и полей» является продолжением алгебраической линейки курсов в первых трёх семестрах. Курс в основном посвящён различным применениям теории колец и полей к классическим задачам математики: великой теореме Ферма, представлениям чисел в виде суммы двух квадратов, основной теореме алгебры, построениям при помощи циркуля и линейки, разрешимости в радикалах. Кроме того, рассматриваются основы алгебраической геометрии, теория конечных полей и нормированные поля.

1. Цели и задачи

Цель дисциплины

освоение основных современных методов теории колец и полей.

Задачи дисциплины

- освоение студентами базовых знаний (понятий, концепций, методов и моделей) в теории колец и полей;
- приобретение теоретических знаний и практических умений и навыков в теории колец и полей;
- оказание консультаций и помощи студентам в проведении собственных теоретических исследований в теории колец и полей.

2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-4 Способен осуществлять сбор и обработку научно-технической и (или) технологической информации для решения фундаментальных и прикладных задач	ОПК-4.4 Владеет навыками работы с компьютером и компьютерными сетями с целью получения, хранения и обработки научной (технической, технологической) информации
ПК-1 Способен ставить, формализовывать и решать задачи, в том числе разрабатывать и исследовать математические модели изучаемых явлений и процессов, системно анализировать научные проблемы, получать новые научные результаты	ПК-1.2 Способен выдвигать гипотезы, строить математические модели для описания изучаемых явлений и процессов, оценивать качество разработанной модели

3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- фундаментальные понятия, законы, теории теории колец и полей;
- современные проблемы соответствующих разделов теории колец и полей;
- понятия, аксиомы, методы доказательств и доказательства основных теорем в разделах, входящих в базовую часть цикла теории колец и полей;
- основные свойства соответствующих математических объектов;
- аналитические и численные подходы и методы для решения типовых прикладных задач теории колец и полей.

уметь:

- понять поставленную задачу;
- использовать свои знания для решения фундаментальных и прикладных задач;
- оценивать корректность постановок задач;
- строго доказывать или опровергать утверждение;
- самостоятельно находить алгоритмы решения задач, в том числе и нестандартных, и проводить их анализ;
- самостоятельно видеть следствия полученных результатов;
- точно представить математические знания в топологии в устной и письменной форме.

владеть:

навыками освоения большого объема информации и решения задач (в том числе, сложных);
 навыками самостоятельной работы и освоения новых дисциплин;
 культурой постановки, анализа и решения математических и прикладных задач, требующих
 для своего решения использования математических подходов и методов;
 предметным языком топологии и навыками грамотного описания решения задач и
 представления полученных результатов.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий

№	Тема (раздел) дисциплины	Трудоемкость по видам учебных занятий, включая самостоятельную работу, час.			
		Лекции	Семинары	Лаборат. работы	Самост. работа
1	Кольцо	2	2		5
2	Евклидовы кольца	2	2		5
3	Подкольца и идеалы	2	2		5
4	Великая теорема Ферма при $n = 3$	2	2		5
5	Факториальность кольца многочленов над факториальным кольцом	4	4		5
6	Нётеровы кольца	2	2		4
7	Расширение поля	4	4		4
8	Алгебраические расширения полей	4	4		4
9	Сепарабельные расширения полей	4	4		4
10	Алгебраическая замкнутость поля комплексных чисел	4	4		4
Итого часов		30	30		45
Подготовка к экзамену		30 час.			
Общая трудоёмкость		135 час., 3 зач.ед.			

4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

Семестр: 4 (Весенний)

1. Кольцо

Определения и свойства делимости

2. Евклидовы кольца

Разложение на простые в евклидовых кольцах

3. Подкольца и идеалы

Подкольцо Идеал. Кольцо главных идеалов. Целые гауссовы числа и числа Эйзенштейна. Контрпримеры. Максимальные и простые идеалы.

4. Великая теорема Ферма при $n = 3$

Теорема о соответствии между подгруппами и промежуточными полями

5. Факториальность кольца многочленов над факториальным кольцом

Поле частных. Факториальность $\mathbb{Z}[x]$. Основная теорема.

6. Нётеровы кольца

Нётеровы кольца

7. Расширение поля

Характеристика поля. Степень расширения поля.

8. Алгебраические расширения полей

Алгебраические элементы и расширения. Алгебраически замкнутое поле.

9. Сепарабельные расширения полей

Теорема о примитивном элементе. Группа Галуа.

10. Алгебраическая замкнутость поля комплексных чисел

Конечные поля. Нормирования. Поле p -адических чисел.

5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Стандартная учебная аудитория.

6. Перечень рекомендуемой литературы

Основная литература

1. Курс алгебры [Текст] : [учебник для вузов] / Э. Б. Винберг .— 2-е изд., стереотип. — М : МЦНМО, 2013 .— 592 с.: ил. - Библиогр.: с. 570-571. - Предм. указ.: с.575-590. - 2000 экз. - ISBN 978-5-4439-0209-8 (в пер.) .— Полный текст (Доступ из сети МФТИ / Удаленный доступ).

Дополнительная литература

1. Введение в алгебру [Текст] : в 3 ч. Ч. 3 : Основные структуры алгебры : учебник для вузов / А. И. Кострикин .— 2-е изд., стереотип. — М. : МЦНМО, 2009, 2012 .— 272 с.

7. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

<http://dm.fizteh.ru/>

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)

На лекционных занятиях используются мультимедийные технологии, включая демонстрацию презентаций.

В процессе самостоятельной работы обучающихся возможно использование таких программных средств, как Mathcad, MATLAB, Maple и др.

9. Методические указания для обучающихся по освоению дисциплины (модуля)

1. Рекомендуется успешно сдавать контрольные работы, так как это упрощает итоговую аттестацию по предмету.
2. Для подготовки к итоговой аттестации по предмету лучше всего пользоваться материалами лекций.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

по направлению: Прикладная математика и информатика
профиль подготовки: Математика
Физтех-школа Прикладной Математики и Информатики
кафедра дискретной математики
курс: 2
квалификация: бакалавр

Семестр, формы промежуточной аттестации: 4 (весенний) - Экзамен

Разработчик: Д.Г. Ильинский, канд. экон. наук, доцент

1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-4 Способен осуществлять сбор и обработку научно-технической и (или) технологической информации для решения фундаментальных и прикладных задач	ОПК-4.4 Владеет навыками работы с компьютером и компьютерными сетями с целью получения, хранения и обработки научной (технической, технологической) информации
ПК-1 Способен ставить, формализовывать и решать задачи, в том числе разрабатывать и исследовать математические модели изучаемых явлений и процессов, системно анализировать научные проблемы, получать новые научные результаты	ПК-1.2 Способен выдвигать гипотезы, строить математические модели для описания изучаемых явлений и процессов, оценивать качество разработанной модели

2. Показатели оценивания компетенций

В результате изучения дисциплины «Теория колец и полей» обучающийся должен:

знать:

фундаментальные понятия, законы, теории теории колец и полей;
современные проблемы соответствующих разделов теории колец и полей;
понятия, аксиомы, методы доказательств и доказательства основных теорем в разделах, входящих в базовую часть цикла теории колец и полей;
основные свойства соответствующих математических объектов;
аналитические и численные подходы и методы для решения типовых прикладных задач теории колец и полей.

уметь:

понять поставленную задачу;
использовать свои знания для решения фундаментальных и прикладных задач;
оценивать корректность постановок задач;
строго доказывать или опровергать утверждение;
самостоятельно находить алгоритмы решения задач, в том числе и нестандартных, и проводить их анализ;
самостоятельно видеть следствия полученных результатов;
точно представить математические знания в топологии в устной и письменной форме.

владеть:

навыками освоения большого объема информации и решения задач (в том числе, сложных);
навыками самостоятельной работы и освоения новых дисциплин;
культурой постановки, анализа и решения математических и прикладных задач, требующих для своего решения использования математических подходов и методов;
предметным языком топологии и навыками грамотного описания решения задач и представления полученных результатов.

3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю

Перечень типовых задач контрольной работы, вопросы для текущего контроля и итоговой аттестации приведены в отдельных файлах. Приложение 1

4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся

Критерии оценивания

- оценка «отлично (10)» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений
- оценка «отлично (9)» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений
- оценка «отлично (8)» выставляется студенту, показавшему всесторонние систематизированные, глубокие знания учебной программы дисциплины и умение применять их на практике при решении конкретных задач, и правильное обоснование принятых решений
- оценка «хорошо (7)» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «хорошо (6)» выставляется студенту, если он знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «хорошо (5)» выставляется студенту, если он знает материал, и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «удовлетворительно (4)» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;
- оценка «удовлетворительно (3)» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет фрагментарно основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;
- оценка «неудовлетворительно (2)» выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач
- оценка «неудовлетворительно (1)» выставляется студенту, который не знает формулировок основных понятий дисциплины.

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Во время проведения экзамена обучающиеся могут пользоваться программой дисциплины.

Везде, где не сказано иного, рассматривается расширение $K \supset F$, а $\alpha \in K$ — алгебраический над K элемент.

Через ξ_n обозначим примитивный корень n -ой степени из 1.

Типовые задачи

Задача 1. Найдите степень расширения $\mathbb{Q}(\alpha)$ (например, $\alpha = \sqrt{2}, \sqrt{2}i, \sqrt[3]{2}, \xi_5, \sqrt{2} + \sqrt{3}, \xi_8$).

Задача 2. Найдите минимальные многочлены для α над F (например, $\sqrt{2}$ над \mathbb{Q} ; $\sqrt[3]{2}$ над \mathbb{Q} ; $\sqrt[7]{5}$ над \mathbb{Q} ; $2 - 3i$ над \mathbb{R} ; $2 - 3i$ над \mathbb{C} ; $\sqrt{2} + \sqrt{3}$ над \mathbb{Q} ; $1 + \sqrt{2}$ над $\mathbb{Q}(\sqrt{2} + \sqrt{3})$).

Задача 3. Найдите степень поля разложения для многочленов (например, $x^2 - 2, x^3 - 2, x^4 - 2, x^5 - 2$).

Задача 4. Найдите примитивный элемент расширения (например $\mathbb{Q}(\sqrt{2})$; $\mathbb{Q}(\sqrt{2}, \sqrt{3})$; $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$).

Задача 5. Является ли данное расширение нормальным?

Задача 6. Найдите группу Галуа данного расширения.

Задача 7. Для конечного поля: построение, нахождение порождающего элемента поля.

Обычные задачи

Задача 8. Многочлен $\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$ (p — простое число) неприводим над \mathbb{Q} .

Задача 9. Многочлен $x^n - p$ (p — простое число) неприводим над \mathbb{Q} .

Задача 10. Любое конечное поле имеет положительную характеристику.

Задача 11. (Нетривиальный) гомоморфизм полей $\varphi : F \rightarrow K$ является инъективным.

Задача 12. У поля F конечной характеристики $\text{char } F$ — простое число.

Задача 13. Любое поле F нулевой характеристики содержит \mathbb{Q} в качестве подполя.

Задача 14. Если существует нетривиальный гомоморфизм полей $\varphi : F \rightarrow K$, то $\text{char } F = \text{char } K$.

Задача 15. Если $K \supset F$ — расширение полей, то K является линейным пространством над F .

Задача 16. Пусть $f(x)$ — неприводимый многочлен степени n , и $K = F[x]/(f(x))$. Тогда многочлен $f(x)$ имеет корень в K .

Задача 17. Пусть $f(x)$ — неприводимый многочлен степени n , и $K = F[x]/(f(x))$. Чему равна степень $[K : F]$ этого расширения?

Задача 18. Верно ли, что для любого многочлена $g(x) \in F[x]$ найдётся расширение поля F , в котором $g(x)$ имеет корень?

Задача 19. Верно ли, что любое конечное расширение поля является алгебраическим?

Задача 20. Верно ли, что у любого поля существует не алгебраическое расширение?

Задача 21. Если α является корнем неприводимого многочлена $f(x)$, то $f(x)$ порождает идеал $m_{\alpha, F} = \{g(x) \in F[x] \mid g(\alpha) = 0\}$.

Задача 22. Пусть $f(x), g(x)$ — неприводимые многочлены со старшим коэффициентом 1, у которых α является корнем. Тогда $f(x) = g(x)$.

Задача 23. Верно ли, что если у K нет нетривиальных алгебраических расширений, то полем разложения любого многочлена $f \in K[x]$ является K ? (Если верно, то докажите это, если неверно, приведите контрпример)

Задача 24. Верно ли, что если полем разложения любого многочлена $f \in K[x]$ является K , то у K нет нетривиальных алгебраических расширений?

Задача 25. Верно ли, что если любой многочлен степени ≥ 1 из $K[x]$ имеет корень в поле K , то у K нет нетривиальных алгебраических расширений?

Задача 26. Верно ли, что если у K нет нетривиальных алгебраических расширений, то любой многочлен степени ≥ 1 из $K[x]$ имеет корень в поле K ?

Задача 27. Верно ли, что над алгебраически замкнутым полем K нет нетривиальных расширений?

Задача 28. Пусть α, β — корни неприводимого многочлена $f(x) \in F[x]$. Тогда поля $F(\alpha)$ и $F(\beta)$ изоморфны.

Задача 29. Назовём число $x \in \mathbb{C}$ алгебраическим, если x алгебраично над \mathbb{Q} . Множество всех алгебраических чисел обозначим через $\overline{\mathbb{Q}}$. Докажите, что $\overline{\mathbb{Q}}$ является полем.

Задача 30. Докажите, что для алгебраических над F элементов α и β следующие условия эквивалентны: $m_{\alpha, F} = m_{\beta, F}$ и $m_{\alpha, F}(\beta) = 0$.

Задача 31. Пусть $\varphi : F \rightarrow F$ — автоморфизм поля F (изоморфизм поля на себя).

а) Пусть $\text{char } F = 0$. Верно ли, что φ сохраняет \mathbb{Q} ? (то есть при $q \in \mathbb{Q}$ выполнено равенство $\varphi(q) = q$).

б) Пусть $\text{char } F = p$. Верно ли, что φ сохраняет \mathbb{Z}_p ?

Задача 32. Пусть $F \subset K$ — расширение полей, $H \subset \text{Aut}_F(K)$ — подгруппа. Тогда $K^H = \{x \in K \mid \forall h \in H \ h(x) = x\}$ является полем, причём $K \supset K^H \supset F$.

Задача 33. Пусть $K \supset L \supset F$ — башня расширений полей, $K \supset F$ — нормальное расширение. Тогда $K \supset L$ — нормальное расширение.

Задача 34. Докажите, что конечное поле характеристики p состоит из p^n элементов.

Задача 35. Существует единственное поле из p^n элементов.

Задача 36. Пусть $f \in \mathbb{Z}_p[x]$ — многочлен, у которого производная равна 0. Тогда

а) $f \in \mathbb{Z}_p[x^p]$;

б) $f = g^p$ для некоторого $g \in \mathbb{Z}_p[x]$.

в) Пусть F — конечное поле. Для неприводимого многочлена $h \in F[x]$ в его поле разложения все корни различны.

Задача 37. Опишите все подполя поля а) \mathbb{F}_{32} ; б) \mathbb{F}_{81} ; в) $\mathbb{F}_{2^{30}}$.

Задача 38. Верно ли, что неприводимый многочлен над \mathbb{F}_p делит многочлен $x^{p^n} - x$ тогда и только тогда, когда его степень делит n ?

Во всех задачах, если не сказано иное, под K подразумевается коммутативное кольцо. Кроме того, будем считать, что $D = \mathbb{Z}[u]$, где $u = i$ или ω .

Типовые задачи

Задача 1. Уметь отвечать на вопросы является ли данное кольцо K коммутативным? ассоциативным? кольцом с единицей? областью целостности? полем? евклидово кольцо? Какие в K есть обратимые элементы? неразложимые? простые?

Задача 2. Для заданного числа $z = a + bu \in D$ с $N(z) \leq 100$ найти разложение z на неразложимые.

Задача 3. Для заданных элементов z_1, z_2 найти порождающий элемент идеала (z_1, z_2) .

Задача 4. Найти факторкольцо $K/(x_1, x_2, x_3)$.

Задачи с семинаров

Задача 5. Для любых $a, b, c \in K$ $a0 = 0a = 0$.

Задача 6. В кольце не может быть двух различных единиц.

Задача 7. Пусть кольцо с единицей содержит не меньше двух элементов. Тогда $1 \neq 0$.

Задача 8. В коммутативном кольце элемент не может иметь двух различных обратных элементов.

Задача 9. Обратимый элемент кольца не может быть делителем нуля.

Задача 10. Если K — кольцо без делителей нуля, то возможно сокращение: если $ac = bc$ (или $ca = cb$) и $c \neq 0$, то $a = b$.

Задача 11. В конечном коммутативном кольце если элемент не является делителем нуля, то он обратим.

Задача 12. Конечная область целостности — поле.

Задача 13. а) Докажите, что для элементов x, y области целостности K следующие условия равносильны: (1) $x \sim y$; (2) $x \mid y$ и $y \mid x$; (3) множество делителей x и множество делителей y равны. б) Отношение \sim является отношением эквивалентности.

Задача 14. Простой элемент области целостности является неразложимым.

Задача 15. Для любого числа $u \in \mathbb{C}$ определим множество $\mathbb{Z}[u] = \cup_{n=0}^{\infty} \{a_0 + a_1u + \dots + a_nu^n \mid a_0, a_1, \dots, a_n \in \mathbb{Z}\}$.

а) Докажите, что $\mathbb{Z}[u]$ является областью целостности. б) При каких $u \in \mathbb{C}$ данное $\mathbb{Z}[u]$ «конечномерно над \mathbb{Z} », то есть найдётся такое N , что $\mathbb{Z}[u] = \{a_0 + a_1u + \dots + a_Nu^N \mid a_0, a_1, \dots, a_n, \dots \in \mathbb{Z}\}$?

Задача 16. Множество K^* обратимых элементов кольца K является группой по умножению. Она называется *мультипликативной группой* или *группой обратимых элементов* кольца K .

Задача 17. K — евклидово кольцо. Верно ли, что если для $a, b \neq 0$ выполнено равенство $N(ab) = N(a)$, то b обратим?

Задача 18. K — евклидово кольцо. Верно ли, что для $a \neq 0, b \in K^*$ выполнено равенство $N(ab) = N(a)$?

Задача 19. Докажите, что для $z \in \mathbb{Z}[i]$ выполнено утверждение $N(z) = 1 \Rightarrow z$ — обратим.

Задача 20. Докажите, что для $z \in \mathbb{Z}[\omega]$ выполнено утверждение $N(z) = 1 \Rightarrow z$ — обратим.

Задача 21. Докажите, что для $z \in \mathbb{Z}[i]$ выполнено утверждение $N(z) = 1 \Leftarrow z$ — обратим.

Задача 22. Докажите, что для $z \in \mathbb{Z}[\omega]$ выполнено утверждение $N(z) = 1 \Leftarrow z$ — обратим.

Задача 23. Если $k \in \mathbb{Z}$, то $z = a + bu \in D$ делится на k тогда и только тогда, когда a и b делятся на k .

Задача 24. Если $z \in D, z \mid x$, и $N(z) = N(x)$, то $z \sim x$.

Задача 25. а) Если z — неразложимый элемент D , то существует такое простое целое число p , что $N(z) = p$ или $N(z) = p^2$.

б) Если z — неразложимый элемент D и $N(z) = p^2$, то z ассоциировано с p .

в) Если $N(z) = p$, то z — неразложимый элемент D .

г) Пусть p — простое целое число. Тогда есть два варианта: либо p неразложимо в D , либо $p = z\bar{z}$, где z — неразложимо в D . Таким образом описываются все неразложимые элементы D .

Задача 26. (*Простые гауссовы числа*) Пусть p — простое целое число.

а) Если $p = 4k + 3$, то p — неразложим в $\mathbb{Z}[i]$.

б) Если $p = 4k + 1$, то p — разложим в $\mathbb{Z}[i]$.

в) Если $p = 4k + 1$, то $p = z\bar{z}$, где z — неразложим в $\mathbb{Z}[i]$.

г) Неразложимые элементы $\mathbb{Z}[i]$, не описанные в предыдущих пунктах — $1 \pm i$.

Задача 27. (*Простые числа Эйзенштейна*) Пусть p — простое целое число.

а) Если $p = 3k + 2$, то p — неразложим в $\mathbb{Z}[\omega]$.

б) Если $p = 3k + 1$, то p — разложим в $\mathbb{Z}[\omega]$.

в) Если $p = 3k + 1$, то $p = z\bar{z}$, где z — неразложим в $\mathbb{Z}[\omega]$.

Задача 28. Пусть $I \subset K$ является подмножеством, для которого выполнено следующее условие: для любых $a \in K, x \in I, y \in I$ верно, что $x + y \in I, ax \in I$. Верно ли что это условие равносильно тому, что I — идеал?

Задача 29. а) Для произвольных элементов x_1, \dots, x_n кольца K множество

$$(x_1, \dots, x_n) = \{a_1x_1 + \dots + a_nx_n \mid a_1, \dots, a_n \in K\}$$

является идеалом. Он называется *идеалом, порождённым элементами* x_1, \dots, x_n .

б) Докажите, что (x_1, \dots, x_n) — минимальный по включению идеал, содержащий элементы x_1, \dots, x_n .

Задача 30. Пусть $I \subset K$ — идеал. Всегда ли *радикал* $\sqrt{I} = \{a \in K \mid \exists m \in \mathbb{N} : a^m \in I\}$ идеала I является идеалом?

Задача 31. Всегда ли множество делителей нуля (с добавлением 0) является идеалом?

Задача 32. Пусть $N(K)$ — множество *нильпотентных элементов* кольца K , то есть элементов, некоторая степень которых равна 0

$$N(K) = \{a \in K \mid \exists n \in \mathbb{N} : a^n = 0\}.$$

Всегда ли $N(K)$ является идеалом?

Задача 33. Пусть $K \neq 0$. Докажите, что K является полем тогда и только тогда, когда K не содержит нетривиальных идеалов.

Утверждения с лекций.

Задача 34. а) Докажите, что $a \mid b$ тогда и только тогда, когда $(b) \subset (a)$. б) Докажите, что $a \sim b$ тогда и только тогда, когда $(a) = (b)$.

Задача 35. Пусть $I, J \subset K$ — идеалы. Докажите, что *сумма* $I + J = \{x + y \mid x \in I, y \in J\}$ и *пересечение* $I \cap J$ идеалов являются идеалами.

Задача 36. Евклидово кольцо является кольцом главных идеалов.

Задача 37. Докажите, что в кольце главных идеалов любой неразложимый элемент является простым.

Задача 38. Докажите, что в кольце главных идеалов любая возрастающая цепочка идеалов

$$(a_1) \subset (a_2) \subset (a_3) \subset \dots \subset (a_n) \subset \dots$$

стабилизируется, то есть найдётся такое k , что $(a_k) = (a_{k+1}) = \dots$.

Задача 39. Пусть $K = \mathbb{Z}[i]$, $x, y \in \mathbb{Z}$. Докажите, что x и y взаимно-просты в \mathbb{Z} тогда и только тогда, когда x и y взаимно просты в $\mathbb{Z}[i]$.

Задача 40. Пусть $K = \mathbb{Z}[i]$, $(x, y) = 1$. Какие значения может принимать $(x + yi, x - yi)$?

Задача 41. Пусть $K = \mathbb{Z}[i]$, $(x, y) = (y, z) = (x, z) = 1$, z — нечётно, выполнено равенство $z^2 = x^2 + y^2$. Тогда $z = m^2 + n^2$ для некоторых $m, n \in \mathbb{Z}$.

Задача 42. Пусть $K = \mathbb{Z}[\omega]$, $\lambda = 1 - \omega$. Докажите, что если $x \in K$ не делится на λ , то $x \equiv r \pmod{3}$, где $r \in K^*$.

Задача 43. Пусть $K = \mathbb{Z}[\omega]$, $\lambda = 1 - \omega$. Докажите, что если $x \in K$ не делится на λ , то $x^3 \equiv \pm 1 \pmod{9}$.

Задача 44. Пусть $K = \mathbb{Z}[\omega]$, $\lambda = 1 - \omega$. Пусть $(x, y) = 1$. Докажите, что $(x + y, x + \omega y) = (x + y, x + \omega^2 y) = (x + \omega y, x + \omega^2 y)$.

Задача 45. Пусть $K = \mathbb{Z}[\omega]$, $\lambda = 1 - \omega$. Пусть $(x, y) = 1$. Докажите, что $(x + y, x + \omega y) = 1$ или λ .

Задача 46. Пусть $K = \mathbb{Z}[\omega]$, $\lambda = 1 - \omega$. Пусть существует нетривиальное решение уравнения $x^3 + y^3 = z^3$. Докажите, что $x y z$ делится на λ .

Во всех задачах, если не сказано иное, под K подразумевается коммутативное кольцо. Кроме того, будем считать, что $D = \mathbb{Z}[u]$, где $u = i$ или ω .

Типовые задачи

Задача 1. Уметь отвечать на вопросы является ли данное кольцо K коммутативным? ассоциативным? кольцом с единицей? областью целостности? полем? евклидово кольцо? Какие в K есть обратимые элементы? неразложимые? простые?

Задача 2. Для заданного числа $z = a + bu \in D$ с $N(z) \leq 100$ найти разложение z на неразложимые.

Задача 3. Для заданных элементов z_1, z_2 найти порождающий элемент идеала (z_1, z_2)

Обычные задачи

Задача 4. Для любых $a, b, c \in K$ $a0 = 0a = 0$.

Задача 5. В кольце не может быть двух различных единиц.

Задача 6. Пусть кольцо с единицей содержит не меньше двух элементов. Тогда $1 \neq 0$.

Задача 7. В коммутативном кольце элемент не может иметь двух различных обратных элементов.

Задача 8. Обратимый элемент кольца не может быть делителем нуля.

Задача 9. Если K — кольцо без делителей нуля, то возможно сокращение: если $ac = bc$ (или $ca = cb$) и $c \neq 0$, то $a = b$.

Задача 10. В конечном коммутативном кольце если элемент не является делителем нуля, то он обратим.

Задача 11. Конечная область целостности — поле.

Задача 12. а) Докажите, что для элементов x, y области целостности K следующие условия равносильны: (1) $x \sim y$; (2) $x \mid y$ и $y \mid x$; (3) множество делителей x и множество делителей y равны. б) Отношение \sim является отношением эквивалентности.

Задача 13. Простой элемент области целостности является неразложимым.

Задача 14. Для любого числа $u \in \mathbb{C}$ определим множество $\mathbb{Z}[u] = \cup_{n=0}^{\infty} \{a_0 + a_1u + \dots + a_nu^n \mid a_0, a_1, \dots, a_n \in \mathbb{Z}\}$.

а) Докажите, что $\mathbb{Z}[u]$ является областью целостности. б) При каких $u \in \mathbb{C}$ данное $\mathbb{Z}[u]$ «конечномерно над \mathbb{Z} », то есть найдётся такое N , что $\mathbb{Z}[u] = \{a_0 + a_1u + \dots + a_Nu^N \mid a_0, a_1, \dots, a_n, \dots \in \mathbb{Z}\}$?

Задача 15. Множество K^* обратимых элементов кольца K является группой по умножению. Она называется *мультипликативной группой* или *группой обратимых элементов* кольца K .

Задача 16. K — евклидово кольцо. Верно ли, что если для $a, b \neq 0$ выполнено равенство $N(ab) = N(a)$, то b обратим?

Задача 17. K — евклидово кольцо. Верно ли, что для $a \neq 0, b \in K^*$ выполнено равенство $N(ab) = N(a)$?

Задача 18. Докажите, что для $z \in \mathbb{Z}[i]$ выполнено утверждение $N(z) = 1 \Rightarrow z$ — обратим.

Задача 19. Докажите, что для $z \in \mathbb{Z}[\omega]$ выполнено утверждение $N(z) = 1 \Rightarrow z$ — обратим.

Задача 20. Докажите, что для $z \in \mathbb{Z}[i]$ выполнено утверждение $N(z) = 1 \Leftarrow z$ — обратим.

Задача 21. Докажите, что для $z \in \mathbb{Z}[\omega]$ выполнено утверждение $N(z) = 1 \Leftarrow z$ — обратим.

Задача 22. Если $k \in \mathbb{Z}$, то $z = a + bu \in D$ делится на k тогда и только тогда, когда a и b делятся на k .

Задача 23. Если $z \in D, z \mid x$, и $N(z) = N(x)$, то $z \sim x$.

Задача 24. а) Если z — неразложимый элемент D , то существует такое простое целое число p , что $N(z) = p$ или $N(z) = p^2$.

б) Если z — неразложимый элемент D и $N(z) = p^2$, то z ассоциировано с p .

в) Если $N(z) = p$, то z — неразложимый элемент D .

г) Пусть p — простое целое число. Тогда есть два варианта: либо p неразложимо в D , либо $p = z\bar{z}$, где z — неразложимо в D . Таким образом описываются все неразложимые элементы D .

Задача 25. (*Простые гауссовы числа*) Пусть p — простое целое число.

а) Если $p = 4k + 3$, то p — неразложим в $\mathbb{Z}[i]$.

б) Если $p = 4k + 1$, то p — разложим в $\mathbb{Z}[i]$.

в) Если $p = 4k + 1$, то $p = z\bar{z}$, где z — неразложим в $\mathbb{Z}[i]$.

г) Неразложимые элементы $\mathbb{Z}[i]$, не описанные в предыдущих пунктах — $1 \pm i$.

Задача 26. (*Простые числа Эйзенштейна*) Пусть p — простое целое число.

а) Если $p = 3k + 2$, то p — неразложим в $\mathbb{Z}[\omega]$.

б) Если $p = 3k + 1$, то p — разложим в $\mathbb{Z}[\omega]$.

в) Если $p = 3k + 1$, то $p = z\bar{z}$, где z — неразложим в $\mathbb{Z}[\omega]$.

Задача 27. Пусть $I \subset K$ является подмножеством, для которого выполнено следующее условие: для любых $a \in K, x \in I, y \in I$ верно, что $x + y \in I, ax \in I$. Верно ли что это условие равносильно тому, что I — идеал?

Задача 28. а) Для произвольных элементов x_1, \dots, x_n кольца K множество

$$(x_1, \dots, x_n) = \{a_1x_1 + \dots + a_nx_n \mid a_1, \dots, a_n \in K\}$$

является идеалом. Он называется *идеалом, порождённым элементами* x_1, \dots, x_n .

б) Докажите, что (x_1, \dots, x_n) — минимальный по включению идеал, содержащий элементы x_1, \dots, x_n .

Задача 29. а) Докажите, что $a \mid b$ тогда и только тогда, когда $(b) \subset (a)$. б) Докажите, что $a \sim b$ тогда и только тогда, когда $(a) = (b)$.

Задача 30. Пусть $I, J \subset K$ — идеалы. Докажите, что *сумма* $I + J = \{x + y \mid x \in I, y \in J\}$ и *пересечение* $I \cap J$ идеалов являются идеалами.

Задача 31. Евклидово кольцо является кольцом главных идеалов.

Задача 32. Докажите, что в кольце главных идеалов любой неразложимый элемент является простым.

Задача 33. Докажите, что в кольце главных идеалов любая возрастающая цепочка идеалов

$$(a_1) \subset (a_2) \subset (a_3) \subset \dots \subset (a_n) \subset \dots$$

стабилизируется, то есть найдётся такое k , что $(a_k) = (a_{k+1}) = \dots$

Правила проведения экзамена по ТКиП - 2020

Аннотация

Курс «Теория колец и полей» является продолжением алгебраической линейки курсов в первых трёх семестрах. Курс в основном посвящён различным применениям теории колец и полей к классическим задачам математики: великой теореме Ферма, представлениям чисел в виде суммы двух квадратов, основной теореме алгебры, построениям при помощи циркуля и линейки, разрешимости в радикалах. Кроме того, рассматриваются основы алгебраической геометрии, теория конечных полей и нормированные поля.

Рейтинг в семестре

В семестре были проведены три контрольные, покрывающие материал листков 1-4, и устные опросы, покрывающие листки 8-13. За каждую контрольную ставится оценка от 0 и до максимума (4 или 5). Это и есть рейтинг в семестре.

Работа на семинарах 1-7 будет добавлена к соотв. контрольным работам.

Зачётная неделя

В течение зачётной недели каждый студент может пересдать либо устный листок 8-13, либо одну из контрольных (также в устном формате).

Если кто-то пропустил контрольные работы: одну контрольную работу можно будет устно пересдать во время зачётной недели.

Как проходит экзамен

Студенты разбиваются на небольшие группы и общаются с преподавателем в течение ~ 2 часов.

Исходя из рейтинга будет (автоматически) сгенерирован список вопросов по темам листков. Чем больше рейтинг, тем сложнее будут вопросы. Чем меньше рейтинг, тем на большее количество вопросов надо будет ответить.

После двух часов ставится оценка от неуд.(2) до отл.(8) включительно. Для желающих получить большую оценку будет проведен дополнительный отдельный опрос.

Устная сдача

Обычно на устной сдаче предъявляются такие требования:

для получения оценки удовл. (3-4) надо знать вопросы на удовл. и основные определения и формулировки утверждений курса. «Знать» означает умение подготовить и обсудить любой вопрос на удовл. с преподавателем за **20** минут.

Оценка хор. (5-7) : знать вопросы на удовл. и хор., а также основные определения и формулировки утверждений курса. Вопросы на удовл. надо уметь отвечать за **15** минут, вопросы на хор. за **20** минут.

Оценка отл. (8-10) : знать все вопросы, а также основные определения и формулировки утверждений курса. Вопросы на удовл. надо уметь отвечать за **10** минут, вопросы на хор. за **15** минут, вопросы на отл. **20** минут.

Для дистанционной сдачи нужно будет рассказывать основные идеи и детали, поэтому время на усмотрение преподавателя может быть сокращено. Например, преподаватель может устроить быстрый опрос на 20-25 минут для выяснения общей оценки, а потом уже дать 2-3 вопроса для уточнения оценки.

Определения

Данный список определений включает не все понятия из курса. Некоторые базовые понятия (поля, характеристика поля, группа) считаются известными из курса алгебры. Другие определения (нётеровы кольца, норма на поле, и.т.п.) нужно уметь формулировать в рамках соответствующего вопроса.

Дать определение = умение не только сформулировать определение, но и дать примеры структур удовлетворяющих/не удовлетворяющих этому определению.

1. Определение коммутативного кольца.
2. Определение обратимого элемента в кольце.
3. Определение делителя нуля в кольце.
4. Определение гомоморфизма колец.
5. Определение области целостности.
6. Определение элемента кольца, ассоциированным с данным элементом.
7. Определение неразложимого элемента области целостности.
8. Определение простого элемента области целостности.
9. Определение евклидова кольца.
10. Определение факториального кольца.
11. Определение чисел Эйзенштейна.
12. Определение наибольшего общего делителя двух элементов области целостности.

13. Определение подкольца в кольце.
14. Определение идеала в кольце.
15. Какие идеалы в кольце называются тривиальными?
16. Определение идеала, порождённого элементами x_1, \dots, x_n .
17. Определение конечно порождённого идеала.
18. Определение главного идеала.
19. Определение кольца главных идеалов.
20. Определение простого идеала.
21. Определение максимального идеала.
22. Определение примитивного многочлена.
23. Определение расширения поля.
24. Определение алгебраического элемента расширения поля.
25. Определение трансцендентного элемента расширения поля.
26. Определение алгебраического расширения поля.
27. Пример алгебраического расширения поля.
28. Пример не алгебраического расширения поля.
29. Определение минимального многочлена элемента расширения поля.
30. Пусть $K \supset F$ — расширение, $\gamma \in K$ — элемент. Что такое $F(\gamma)$?
31. Определение поля разложения многочлена
32. Что значит построить элемент $z \in \mathbb{C}$ при помощи циркуля и линейки.
33. Определение ξ_n — примитивного корня n -ой степени из 1.
34. Определение сопряжённого элемента к данному элементу из $K \supset F$.
35. Сформулируйте критерий неприводимости Эйзенштейна.
36. Определение группы автоморфизмов $\text{Aut}_F K$ расширения $K \supset F$.
37. Определение поля K^H для подгруппы автоморфизмов $H \subset \text{Aut}_F K$ расширения $K \supset F$.
38. Определение нормального расширения.

Везде, где не сказано иного, рассматривается коммутативное кольцо K или расширение $K \supset F$, а $\alpha \in K$ — алгебраический над K элемент. Также подразумевается, что $D = \mathbb{Z}[u]$, где $u = i, \omega, \sqrt{2}i, \sqrt{3}i$ или $2i$.

В скобках после формулировки вопроса может быть указана задача из листка, на которую данный вопрос опирается или ссылается.

Если в пункте сформулировано утверждение, то его надо доказать.

Вопросы на удовл.(3-4)

1. (1.1) Для любых $a, b, c \in K$ а) $a0 = 0a = 0$; б) $a(-b) = (-a)b = -ab$; в) $a(b - c) = ab - ac$ и $(a - b)c = ac - bc$.
2. (1.2)
 - а) В кольце не может быть двух различных единиц.
 - б) Пусть кольцо с единицей содержит не меньше двух элементов. Тогда $1 \neq 0$.
 - в) Может ли элемент ассоциативного кольца иметь более одного обратного элемента?
3. Множество K^* обратимых элементов кольца K является группой по умножению. Она называется *мультипликативной группой* или *группой обратимых элементов* кольца K .
4. (1.3, 2.4) Уметь отвечать на вопросы: является ли данное кольцо K коммутативным? областью целостности? полем? Какие в K есть обратимые элементы? неразложимые? Здесь $K = \mathbb{Z}, \mathbb{Z}[\frac{1}{p}], \mathbb{Q}_p$.
5. (1.6) Обратимый элемент кольца не может быть делителем нуля.
6. (1.6) Если K — кольцо без делителей нуля, то возможно сокращение: если $ac = bc$ (или $ca = cb$) и $c \neq 0$, то $a = b$.
7. (1.7-1.9) Базовые знания про комплексные числа: сложение, умножение, модуль, аргумент, извлечение корней n -ой степени.
8. (1.18) Нарисуйте на комплексной плоскости *целые гауссовы числа* $\mathbb{Z}[i]$ и найдите $\mathbb{Z}[i]^*$.
9. (2.1) Для всех $a, b, c \in K$ выполнено: $a \mid a$; $a \mid 0$; если $a \mid b$ и $b \mid c$, то $a \mid c$; если $a \mid c$ и $a \mid b$, то $a \mid (b + c)$.
10. (2.2) а) Докажите, что для элементов x, y области целостности K следующие условия равносильны: (1) $x \sim y$; (2) $x \mid y$ и $y \mid x$; (3) множество делителей x и множество делителей y равны. б) Отношение \sim является отношением эквивалентности.
11. (2.8) В евклидовом кольце $N(ab) = N(a)$ тогда и только тогда, когда b обратим.
12. (2.13) Любой простой элемент неразложим.

13. (3.3) Для $u = i, \omega$ и простого целого числа $p \leq 40$ выясните, существует ли $z \in \mathbb{Z}[u]$ с $N(z) = p$. Сформулируйте гипотезу о том, какие простые целые числа являются простыми в $\mathbb{Z}[u]$.
14. (3.7) Умение находить НОД для евклидова кольца D .
15. (3.4ab)
- а) Если p — простое целое число и существует такое $z \in D$, что $N(z) = p$, то z — неразложимый элемент.
- б) Если p — простое целое число и не существует такого $z \in D$, что $N(z) = p$, то p — неразложимый элемент.
16. (4.1)
- а) $0 \subset K, K \subset K$ — идеалы. Они называются *тривиальными*.
- б) $(a) = \{ax \mid x \in K\}$ — *главный идеал* или *идеал, порождённый одним элементом*
- в) $(a_1, \dots, a_n) = \{a_1x_1 + \dots + a_nx_n \mid x_1, \dots, x_n \in K\}$ — *конечно-порождённый идеал*, то есть идеал, порождённый конечным количеством элементов.
17. (4.2) Пусть $I \subset K$ является подмножеством, для которого выполнено следующее условие: для любых $a \in K, x \in I, y \in I$ верно, что $x + y \in I, ax \in I$. Верно ли что это условие равносильно тому, что I — идеал?
18. (4.3) а) Докажите, что $a \mid b$ тогда и только тогда, когда $(b) \subset (a)$. б) Докажите, что $a \sim b$ тогда и только тогда, когда $(a) = (b)$.
19. (4.5) Пусть $I, J \subset K$ — идеалы. Докажите, что *сумма* $I + J = \{x + y \mid x \in I, y \in J\}$ и *пересечение* $I \cap J$ идеалов являются идеалами.
20. (4.6б) Пусть K — коммутативное кольцо. Является ли идеалом множество делителей нуля кольца K с добавленным 0?
21. (4.11) Пусть $K \neq 0$. Докажите, что K является полем тогда и только тогда, когда K не содержит нетривиальных идеалов.
22. (5.1) Верно ли, что при гомоморфизме колец $\varphi : K \rightarrow L$ а) образ идеала $I \subset K$ является идеалом в L ; б) образ $I \subset K$ является идеалом в $\varphi(K)$; в) прообраз идеала $J \subset L$ является идеалом в K ?
23. (5.2) а) Всегда ли факторкольцо коммутативного кольца является коммутативным кольцом? б) Имеется *канонический* гомоморфизм $\varphi : K \rightarrow K/I$, который переводит $a \mapsto a + I$.
24. (5.6) Пусть $J \subset I \subset K$ — цепочка вложенных идеалов в кольце K . Тогда кольцо $(K/J)/(I/J)$ изоморфно K/I .
25. (5.7, 5.10) Умение находить факторкольца/ максимальные/простые идеалы.
26. (5.8) Пусть K — область целостности. Идеал (x) является простым тогда и только тогда, когда x прост.
27. (5.8) Пусть K — область целостности. Нетривиальный идеал I является простым тогда и только тогда, когда K/I область целостности.
28. (5.8) Пусть K — область целостности. Нетривиальный идеал I является максимальным тогда и только тогда, когда K/I поле.
29. (5.8) В кольце главных идеалов любой простой идеал максимален.
30. (5.9) Является ли кольцо $\mathbb{Z}[x]$ евклидовым?
31. (8.1) Пусть K — область целостности. Рассмотрим множество пар $\tilde{K} = \{a, b\}$ элементов кольца K , где $b \neq 0$. На этом множестве введем отношение следующим образом: $\{a, b\} \sim \{c, d\}$, если $ad = bc$.
- а) $\{a, b\} \sim \{ac, bc\}$. б) \sim — отношение эквивалентности. Элемент множества классов эквивалентности $F = \text{Quot}(K)$ будем записывать как $\frac{a}{b}$ или ab^{-1} . Введем операции сложения и умножения на $F = \text{Quot}(K)$:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

- в) Сложение и умножение корректно определено;
- г) F является коммутативным кольцом;
- д) F является полем;
- е) существует инъекция $K \rightarrow F$.
32. (8.3) Нахождение поля частных для конкретных колец.
33. (8.7a) Если несократимая рациональная дробь $\frac{c}{d}$ является корнем $f(x)$, то $c \mid a_0, d \mid a_n$.
34. (8.8a-жс) Применение признака неприводимости Эйзенштейна.
35. (8.9) Какие многочлены степени 0 а) неприводимы; б) являются простыми элементами в $\mathbb{Z}[x]$?

36. (8.11аб)

а) Произведение примитивных многочленов примитивно.

б) Пусть f — примитивный многочлен из $\mathbb{Z}[x]$. Если $f(x)$ неприводим в $\mathbb{Q}[x]$, то он неприводим и в $\mathbb{Z}[x]$.

37. (9.1-9.5)

а) У поля F конечной характеристики $\text{char } F$ — простое число.

б) Если существует нетривиальный гомоморфизм полей $\varphi : F \rightarrow K$, то $\text{char } F = \text{char } K$.

в) Любое конечное поле имеет положительную характеристику.

г) Существует ли бесконечное поле положительной характеристики?

д) (Нетривиальный) гомоморфизм полей $\varphi : F \rightarrow K$ является инъективным

е) Если $K \supset F$ — расширение полей, то K является линейным пространством над F .

38. (9.8, 9.10, 10.4а, 10.8а 11.1) Умение находить степень расширения, минимальный многочлен для алгебраического над полем элемента/ поле разложение многочлена.

39. (10.2) Для башни расширений полей $K \supset L \supset F$ верна формула: $[K : L] \cdot [L : F] = [K : F]$.

40. (10.3)

а) Верно ли, что $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \cong \mathbb{Q}(\sqrt{2})[\sqrt{3}] \cong \mathbb{Q}[\sqrt{2}, \sqrt{3}]$?

б) Какова степень расширения $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})]$?

в) Какова степень расширения $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$?

г) Рассмотрим число $\alpha = \sqrt{2} + \sqrt{3}$. Найдите минимальный многочлен $m_{\alpha, \mathbb{Q}}$.

д) Существует ли такой элемент $\beta \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, что $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$?

41. (10.6) Для каждого многочлена $f(x) \in F[x]$ существует конечное расширение $K \supset F$, в котором $f(x)$ имеет корень.

42. (11.2) а) Сколько имеется примитивных корней степени n ? б) Найдите минимальный многочлен для ξ_n при $n \leq 6$. в) Найдите минимальный многочлен для ξ_n для простого числа n .

43. (11.3) Любое конечное расширение — алгебраическое.

44. (12.1) Докажите, что при помощи циркуля и линейки можно построить

а) все точки с рациональными координатами;

б) ξ_n , где $n = 3, 4, 6$;

Если мы построили точки z, w , то можно ли построить точки в) $\bar{z}, -z$? г) $z + w, z - w$? д) $z \cdot w$.

45. (12.2) Точку $z \in \mathbb{C}$ можно построить тогда и только тогда, когда можно построить точки $\text{Re } z, \text{Im } z$.

46. (12.3) Докажите невозможность удвоения куба, то есть построение куба объёма 2, имея куб объёма 1 с помощью циркуля и линейки.

47. (12.7) Пусть P — некоторое подмножество точек комплексной плоскости. Назовём *точечным полем* для P минимальное расширение $L \supset \mathbb{Q}$, $L \subset \mathbb{C}$, которое содержит обе координаты всех точек из P . Пусть точка $z = x + y \cdot i$ получается при помощи операции пересечения прямых/окружностей из множества точек P . Тогда x, y лежат в расширении точечного поля L для точек P степени не больше, чем 2. Покажите это в случае, когда мы а) пересекаем две прямые; б) пересекаем прямую и окружность; в) пересекаем две окружности.

48. (13.1) Элементы α и β сопряжены над F тогда и только тогда, когда $m_{\alpha, F}(\beta) = 0$.

49. Какие есть элементы, сопряжённые к а) $\sqrt{2}$; б) $\sqrt[3]{2}$; в) $\sqrt{2} + \sqrt{3}$; г) ξ_p для простого p над \mathbb{Q} ?

50. (13.2) Пусть $L \supset F$ — конечное расширение полей. Тогда любой гомоморфизм $\varphi : L \rightarrow L$, сохраняющий F (то есть для любого $a \in F$ выполнено равенство $\varphi(a) = a$) является изоморфизмом на себя, т.е. *автоморфизмом*.

51. (13.3) Пусть $\varphi : F \rightarrow F$ — *автоморфизм поля* F (изоморфизм поля на себя).

а) Пусть $\text{char } F = 0$. Верно ли, что φ сохраняет \mathbb{Q} ? (то есть при $q \in \mathbb{Q}$ выполнено равенство $\varphi(q) = q$).

б) Пусть $\text{char } F = p$. Верно ли, что φ сохраняет \mathbb{Z}_p ?

Пусть теперь $F \supset \mathbb{Q}$.

в) Если $\alpha \in F$ — корень многочлена $f(x) \in \mathbb{Q}[x]$, то $\varphi(\alpha)$ также корень многочлена $f(x)$.

г) Алгебраические элементы при автоморфизмах переходят в сопряжённые (над \mathbb{Q}) элементы.

52. (13.4) а) Пусть α, β — сопряжённые над полем F элементы, $\beta \in F(\alpha)$. Тогда существует единственный автоморфизм $F(\alpha) \rightarrow F(\alpha)$, сохраняющий F и переводящий α в β .

б) Количество автоморфизмов $F(\alpha)$, сохраняющих F , равно количеству сопряжённых (над F) к α элементов, лежащих внутри $F(\alpha)$.

53. (13.5, 7) Опишите группы автоморфизмов и соответствие между промежуточными полями и подгруппами а) $\mathbb{Q}(\sqrt{2})$; б) $\mathbb{Q}(\sqrt[3]{2})$, в) $\mathbb{Q}(\sqrt{2} + \sqrt{3})$.

54. (13.6) Пусть $F \subset K$ — расширение полей. Множество автоморфизмов K , оставляющих F на месте является группой и называется *группой автоморфизмов* и обозначается $\text{Aut}_F(K) = \text{Aut}([K : F])$. Если F — основное поле (\mathbb{Q} или \mathbb{Z}_p), то символ F опускают.

а) $\text{Aut}_F(K)$ — группа.

б) Пусть $H \subset \text{Aut}_F(K)$ — подгруппа. Тогда $K^H = \{x \in K \mid \forall h \in H \ h(x) = x\}$ является полем, причём $K \supset K^H \supset F$.

Вопросы на хор.(5-7)

1. Все умения, указанные в вопросах на удовл., но большей сложности (в разумных пределах).

2. (1.3, 2.7) Уметь отвечать на вопросы: является ли данное кольцо K коммутативным? областью целостности? полем? Какие в K есть обратимые элементы? неразложимые при $|z| < 5$? Здесь $K = \mathbb{Z}[i]$, $\mathbb{Z}[2i]$, $\mathbb{Z}[\sqrt{3}i]$, $\mathbb{Z}[\omega]$.

3. (1.4) Для любого числа $u \in \mathbb{C}$ определим множество $\mathbb{Z}[u] = \bigcup_{n=0}^{\infty} \{a_0 + a_1u + \dots + a_nu^n \mid a_0, a_1, \dots, a_n \in \mathbb{Z}\}$.

а) Докажите, что $\mathbb{Z}[u]$ является областью целостности. **б)** При каких $u \in \mathbb{C}$ данное $\mathbb{Z}[u]$ «конечномерно над \mathbb{Z} », то есть найдётся такое N , что $\mathbb{Z}[u] = \{a_0 + a_1u + \dots + a_Nu^N \mid a_0, a_1, \dots, a_N \in \mathbb{Z}\}$?

4. (1.6) В конечном коммутативном кольце если элемент не является делителем нуля, то он обратим.

5. (1.6) Конечная область целостности (состоящая из более чем одного элемента) — поле.

6. (1.18) **а)** Нарисуйте на комплексной плоскости числа Эйзенштейна $\mathbb{Z}[\omega]$. **б)** Выразите модуль числа $a + b\omega$ через a и b . **в)** Найдите $\mathbb{Z}[\omega]^*$.

7. (2.7) Пример нефакториального кольца вида $\mathbb{Z}[u]$.

8. (2.9) Условие $N(ab) = N(a)N(b)$ из определения евклидова кольца не существенно, то есть область целостности, в которой есть норма с условием делимости с остатком, является евклидовым кольцом.

9. (2.10) (Геометрическое доказательство евклидовости)

а) Нарисуйте точки D на комплексной плоскости.

б) Пусть $a, b \in D$, $b \neq 0$. Пусть q — ближайшая точка решётки D к числу $\frac{a}{b}$. Тогда q — частное при делении a на b с остатком. Как найти r ?

в) Докажите, что $r = 0$ или $N(r) < N(b)$.

10. (2.11) (Алгебраическое доказательство евклидовости) Пусть $a, b \in D$, $b \neq 0$. Тогда $\frac{a}{b}$ можно записать в виде $\alpha + \beta u$, где $\alpha, \beta \in \mathbb{Q}$.

а) Рассмотрев ближайшие целые к α и β , найдите частное q и остаток r от деления a на b .

б) Докажите, что $r = 0$ или $N(r) < N(b)$.

11. (2.12) Пусть K — евклидово кольцо. Тогда **а)** Алгоритм Евклида в K остановится. **б)** Последний не нулевой элемент r_n в алгоритме Евклида — делитель a и b . **в)** Найдутся такие $x, y \in K$, что $r_n = ax + by$. **г)** Определим *наибольший общий делитель* a и b как делитель a и b максимальной нормы. Тогда r_n — наибольший общий делитель

12. (2.14) В факториальном кольце любой неразложимый элемент является простым.

13. (2.15) Если в области целостности K существует разложение в произведение неразложимых элементов и любой неразложимый элемент прост, то K факториально.

14. (2, теорема 1) Евклидово кольцо факториально.

15. (3.4) Если D — факториальное кольцо, то для любого неразложимого элемента $z \in D$ либо $N(z) = p$, либо $z \sim p$ для некоторого целого простого числа p .

16. (3.5, 3.7, 3.9) Следующие простые натуральные числа являются неразложимыми: **а)** числа вида $p = 4k + 3$ в $\mathbb{Z}[i]$; **б)** числа вида $p = 3k + 2$ в $\mathbb{Z}[\omega]$. **в)** числа вида $p \equiv -1, -3 \pmod{8}$ в $\mathbb{Z}[\sqrt{2}i]$.

17. (4.5) Пусть $D = \mathbb{Z}[i]$ или $\mathbb{Z}[\omega]$. **а)** Верно ли, что из $a \mid b$ следует, что $N(a) \mid N(b)$? **б)** Верно ли, что из $(N(a), N(b)) = 1$, следует $(a, b) = 1$? **в)** Пусть $(N(a), N(b)) = p$ — простое целое число, причём $p \nmid a$, $p \nmid b$. Тогда p — разложим, и если $p = z\bar{z}$, то либо z , либо \bar{z} порождает идеал (a, b) , либо z делит одно из этих чисел, а \bar{z} — другое.

18. (4.6ав) Пусть K — коммутативное кольцо. Являются ли идеалом:

а) множество *нильпотентных элементов* $N(K) = \{a \in K \mid \exists m \in \mathbb{N} : a^m = 0\}$;

б) *радикал* $\sqrt{I} = \{a \in K \mid \exists m \in \mathbb{N} : a^m \in I\}$ идеала I ?

19. (4.7) **а)** Идеал (x, y) кольца $\mathbb{Q}[x, y]$ конечно порождён, но не является главным. **б)** Приведите пример области целостности K и идеала I , который не конечно порождён.

20. (4.8) Евклидово кольцо является кольцом главных идеалов.

21. (4.9) Пусть K — кольцо главных идеалов.

а) Любая цепочка возрастающих идеалов стабилизируется, то есть из того, что $I_1 \subset I_2 \subset I_3 \subset \dots \subset I_n \subset \dots$ (где все I_k — идеалы) следует, что найдётся такое n , что $I_n = I_{n+1} = \dots$

- б) В K существует разложение в произведение неразложимых (в смысле 1-й части определения факториального кольца).
22. (4.10) Пусть K — кольцо главных идеалов, p — неразложимый элемент K , ab делится на p , a не делится на p . Рассмотрим I — множество таких элементов $x \in K$, что ax делится на p .
- а) I — идеал.
 б) $1 \notin I$, $p \in I$, $b \in I$.
 в) $I = (p)$.
 г) b делится на p .
 д) Любой неразложимый элемент K является простым.
23. (8.5) а) Верно ли, что $\text{Quot}(\text{Quot}(K)) \cong \text{Quot}(K)$? б) Пусть $K \subset L \subset \text{Quot}(K)$. Верно ли, что $\text{Quot}(K) \cong \text{Quot}(L)$?
24. (8.6) Признак неприводимости Эйзенштейна (формулировка + доказательство)
25. (8.7) Верно ли, что если $f(x)$ неприводим над \mathbb{Z}_p для некоторого простого p , то он неприводим над \mathbb{Q} ?
26. (8.8) Умение применять критерий Эйзенштейна (в том числе, используя замену переменной)
27. (8.11)
 а) Пусть f — примитивный многочлен из $\mathbb{Z}[x]$. Если $f(x)$ неприводим в $\mathbb{Z}[x]$, то он неприводим и в $\mathbb{Q}[x]$.
 б) Примитивный неприводимый многочлен $f \in \mathbb{Z}[x]$ является простым элементом этого кольца.
28. (9.7) а) $F(\alpha_1, \dots, \alpha_n)$ корректно определено. б) Верно ли, что $F(\alpha_1, \dots, \alpha_n) \cong \text{Quot } F[\alpha_1, \dots, \alpha_n]$?
29. (9.9, 10.1) а) Для данного элемента $\alpha \in K$ и многочлена f со старшим коэффициентом 1 следующие условия эквивалентны:
 (1) f порождает идеал $M_\alpha = M_{\alpha, F} = \{f(x) \in F[x] \mid f(\alpha) = 0\}$;
 (2) f — многочлен из M_α минимальной степени;
 (3) f — неприводимый многочлен из M_α .
 б) m_α — единственный многочлен, обладающий данными свойствами;
 в) $F(\alpha) \cong F[\alpha] \cong F[x]/(m_\alpha)$. г) $[F(\alpha) : F] = \deg m_\alpha$.
30. (10.1) Эквивалентность двух определений алгебраического элемента.
31. (10.5) а) Если $\alpha_1, \dots, \alpha_k$ — алгебраические над F элементы, то

$$F(\alpha_1, \dots, \alpha_k) = F[\alpha_1, \dots, \alpha_k].$$

- б) $F[\alpha_1, \dots, \alpha_k] \supset F$ — конечное расширение степени не больше, чем $m_{\alpha_1} \cdot \dots \cdot m_{\alpha_k}$.
 в) Любое конечное расширение $K \supset F$ имеет вид $K = F[\alpha_1, \dots, \alpha_k]$ для некоторых алгебраических над K элементов $\alpha_1, \dots, \alpha_k$.
32. (10.7) Поле разложения многочлена $f(x) \in F[x]$ называется минимальное по включению расширение F , в котором $f(x)$ раскладывается на линейные множители. Поле разложения существует и имеет степень не больше $n!$.
33. (11.5) Назовём число $x \in \mathbb{C}$ алгебраическим, если x алгебраично над \mathbb{Q} . Множество всех алгебраических чисел обозначим через L . Докажите, что L является а) полем; б) алгебраически замкнутым полем; в) $L = \overline{\mathbb{Q}}$.
34. (11.7) Пусть F — конечное поле или поле рациональных чисел.
 а) Можно занумеровать все неприводимые над K многочлены $f_1, f_2, \dots, f_n, \dots$.
 б) Имеется цепочка вложений $F = F_0 \subset F_1 \subset F_2 \subset \dots$, где F_n — поле разложение многочлена f_n над F_{n-1} .
 в) Множество $\tilde{F} = \bigcup_{i=0}^{\infty} F_i$ является полем.
 г) \tilde{F} — алгебраически замкнутое поле.
 д) $\tilde{F} = \overline{F}$ — алгебраическое замыкание F .
35. (12.3) Докажите невозможность трисекции угла, то есть разделения угла в 60° на три части с помощью циркуля и линейки.
36. (12.4) Какие правильные n -угольники можно построить для $3 \leq n \leq 20$?
37. (12.5) Если построены точки x_1, \dots, x_n , то можно построить и любую точку
 а) поля $\mathbb{Q}(x_1, \dots, x_n)$;
 б) поля $K \supset \mathbb{Q}(x_1, \dots, x_n)$, где K — квадратичное расширение поля $\mathbb{Q}(x_1, \dots, x_n)$.
38. (13.4) Пусть $\varphi : F \rightarrow F'$ — изоморфизм полей, γ — алгебраический над F элемент, γ' — корень многочлена $\varphi(m_{\gamma, F})$. Тогда существует единственный изоморфизм полей $F(\gamma) \rightarrow F'(\gamma')$, который переводит γ в γ' и продолжает изоморфизм φ .

39. (13.8) (Группа автоморфизмов $\mathbb{Q}[\sqrt[3]{2}, \omega]$.) Положим $K = \mathbb{Q}[\sqrt[3]{2}, \omega]$. Как мы знаем, K — поле разложения многочлена $f(x) = x^3 - 2$.

а) Пусть $g \in \text{Aut}(K)$. Какие значения может принимать $g(\sqrt[3]{2})$?

б) Элемент $\text{Aut}(K)$ однозначно задаётся перестановкой корней многочлена $f(x)$.

в) Группа $\text{Aut}(K)$ изоморфна S_3 .

г) Рассмотрим подгруппу $A_3 \subset S_3$. Найдите поле K^{A_3} .

д) Рассмотрим три подгруппы H , каждая из которых порождена одной транспозицией. Найдите K^H для каждой такой подгруппы

е) Расширение K имеет четыре нетривиальных подполя, причём эти поля соответствуют подгруппам S_3 . Более того, нормальным подгруппам $H \subset S_3$ соответствуют нормальные расширения $K^H \supset \mathbb{Q}$.

Вопросы на отл.(8).

1. (3.11) Описание представления натурального числа в виде суммы двух квадратов.

2. (3.11-13) Описание пифагоровых троек, используя гауссовы числа.

3. (d1,1-4) Теорема Ферма при $n = 3$ (формулировка). Описание свойств элемента $\lambda = 1 - \omega \in \mathbb{Z}[\omega]$: сравнимость по модулю $\lambda, \lambda^2, \lambda^4$. Если λ делит $x^3 + y^3$ для взаимно-простых x, y , то $(x + y, x + \omega y) = (x + y, x + \omega^2 y) = (x + \omega^2 y, x + \omega y) = \lambda$.

4. (d1,5-6) Теорема Ферма при $n = 3$ (формулировка). Свойства элемента λ (задачи d1,1-4,6/д). Сведение к решению уравнения $x^3 + y^3 = r\lambda^{3k}z^3$ при $k \geq 2$, где $x, y, z \in \mathbb{Z}[\omega]$ — взаимно-простые, $\lambda \nmid xyz$, $r \in \mathbb{Z}[\omega]^*$.

5. (d1,6-7) Теорема Ферма при $n = 3$ с использованием чисел Эйзенштейна (формулировка). Метод спуска (свойствами λ (задачи 1-4) и леммой про сведение к уравнению упрощенного вида (задача 5) можно пользоваться б/д).

6. (6.6) Доказательство эквивалентности определений (4 штуки) нётеровых колец.

7. (6.7) Теорема Гильберта о базисе (нётеровости кольца многочленов над нётеровым кольцом).

8. Если кольцо K факториально, то $K[x]$ тоже факториально.

9. (11.1) Теорема о примитивном элементе.

10. (11.4) Понятие алгебраической замкнутости и алгебраического замыкания поля. Эквивалентность различных определений (6 штук) алгебраически замкнутого поля

11. (11.6) **а)** Пусть $K \supset F$ — алгебраическое расширение, причём любой многочлен из $F[x]$ раскладывается в K на линейные сомножители. Тогда $K = \overline{F}$. **б)** Пусть $F \subset K$, K — алгебраически замкнутое поле. Тогда элементы поля K , алгебраические над F , образуют алгебраически замкнутое поле L .

12. (12, теорема 1) Теорема о построимости комплексного числа при помощи циркуля и линейки.

13. (13.9) Описание группы Галуа $\text{Aut}(K)$ поля K разложения многочлена

а) $x^4 - 2$;

б) $x^4 + 2$ (и похожих). Соответствие подполя K — подгруппы $\text{Aut}(K)$ с уточнением о нормальности.

14. (лекции) Эквивалентность определений нормального расширения (расширения Галуа).

15. (лекции) Основная теорема теории Галуа (формулировка). Доказательство существования биекции между промежуточными полями и подгруппами группы автоморфизмов.

16. (лекции) Основная теорема теории Галуа (формулировка). Уточнение для нормальных подгрупп.

17. (лекции) Теорема о минимальном многочлене примитивного корня n -ой степени из 1. Построимость правильного n -угольника при помощи циркуля и линейки (док-во через теорию Галуа).

18. (лекции) Основная теорема алгебры (доказательство через теорию Галуа).

19. (лекции) Конечные поля. Единственность поля из p^n элементов.

20. (лекции) Конечные поля. Автоморфизм Фробениуса. Описание группы автоморфизмов поля из p^n элементов и соответствия между промежуточными полями и подгруппами этой группы.