Министерство образования Республики Беларусь

Учебно-методическое объединение высших учебных заведений Республики Беларусь по естественнонаучному образованию

УТВЕРЖДАЮ
Первый заместитель Министра образования Республики Беларусь
_____ А.И. Жук
24.09.2008
(дата утверждения)
Регистрационный № ТД-Г.151 /тип.

ГЕОМЕТРИЯ И АЛГЕБРА

Типовая учебная программа для высших учебных заведений по специальности:

1-31 03 04 Информатика

СОГЛАСОВАНО
Председатель Учебно-методического объединения вузов Республики Беларусь по естественнонаучному образованию
_____ В.В. Самохвал
_____
(дата)

СОГЛАСОВАНО
Начальник Управления высшего и среднего специального образования
_____ Ю.И. Миксюк
24.09.2008
(дата)

Первый проректор Государственного учреждения образования «Республиканский институт высшей школы»
_____ В.И. Дынич
25.08.08
(дата)

Эксперт-нормоконтролер
_____ С.М. Артемьева
25.08.08
(дата)

Минск 2008

СОСТАВИТЕЛИ:
Г.П. Размыслович, доцент кафедры высшей математики Белорусского государственного университета, кандидат физико-математических наук, доцент;
А.В. Филипцов, доцент кафедры высшей математики Белорусского государственного университета, кандидат физико-математических наук, доцент;
В.М. Ширяев, доцент кафедры высшей математики Белорусского государственного университета, кандидат физико-математических наук, доцент

РЕЦЕНЗЕНТЫ:
Кафедра высшей математики Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»;
В.В.Шлыков, заведующий кафедрой алгебры и геометрии Учреждения образования «Белорусский государственный педагогический университет им. М. Танка», доктор педагогических наук, профессор

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ В КАЧЕСТВЕ ТИПОВОЙ:
Кафедрой высшей математики Белорусского государственного университета
(протокол № 11 от 20 марта 2008 г.)

Научно-методическим советом Белорусского государственного университета
(протокол № 3 от 27 марта 2008 г.);

Научно-методическим советом по прикладной математике и информатике Учебно-методического объединения вузов Республики Беларусь по естественнонаучному образованию
(протокол № 3 от 24 июня 2008 г.)

Ответственный за выпуск: Г.П. Размыслович

Пояснительная записка

Курс «Геометрия и алгебра» знакомит студентов с основными понятиями аналитической геометрии, линейной и высшей алгебры, прикладной алгебры.

Базой для изучения данного курса является дисциплины «Алгебра» и «Геометрия», изучаемые в средней школе.

Предмет «Геометрия и алгебра» является базовым математическим курсом и непосредственно связан с основными дисциплинами аналитического цикла, такими как «Математический анализ» и «Дифференциальные уравнения». Методы, излагаемые в курсе геометрии и алгебры, используются при изучении дисциплин «Вычислительные методы алгебры», «Теория вероятностей и математическая статистика», «Методы численного анализа», «Функциональный анализ и интегральные уравнения», «Методы оптимизации», а также при изучении ряда дисциплин специализаций.

Основными целями курса являются:

– во-первых, дать глубокие знания по одному из основных разделов курса высшей математики, имеющего тесную связь с многочисленными прикладными проблемами и богатые приложения;

– во-вторых, создать фундаментальные основы, необходимые для усвоения материала перечисленных выше дисциплин;

– в-третьих, сформировать одну из основных частей банка знаний специалистов университетского уровня в избранной области деятельности.

При изложении курса важно показать возможности использования аппарата геометрии и алгебры при решении как чисто теоретических, так и прикладных задач, возникающих в различных областях науки, техники, экономики и др. Целесообразно выделить моменты построения алгоритмов полученных результатов с целью их реализации при помощи средств вычислительной техники.

В результате изучения дисциплины студент должен

знать:

– основы аналитической геометрии плоскости и пространства;
– основные понятия высшей алгебры;
– основы линейной алгебры;
– основы теорий чисел, групп, колец, полей и их приложения к вопросам защиты информации;

уметь:

– применять метод координат при исследовании алгебраических кривых и поверхностей первого и второго порядков;
– решать основные задачи теории векторных, евклидовых и унитарных пространств;
– анализировать и применять основные криптосистемы и коды;
– применять аппарат аналитической геометрии, линейной алгебры, теорий чисел групп, колец, полей при решении задач специальности.

В соответствии с типовым учебным планом специальности 1-31 03 04 «Информатика» учебная программа предусматривает для изучения дисциплины 637 учебных часов, в том числе 340 аудиторных часов: лекции – 170 часов, практические занятия – 170 часов.

Примерный тематический план

№	Название раздела, темы	Количество аудиторных часов		
		Всего	В том числе	
			Лекции	Практические занятия
	Введение.	1	1	
	Раздел 1. Аналитическая геометрия на плоскости и в пространстве.			
1.	Системы координат на прямой, плоскости и пространстве.	5	3	2
2.	Векторы.	16	8	8
3.	Прямые и плоскости.	22	10	12
4.	Фигуры второго порядка на плоскости и в пространстве.	20	10	10
	Раздел 2. Алгебра.			
5.	Алгебраическая операция. Группа, кольцо, поле.	8	4	4
6.	Комплексные числа.	12	6	6
7.	Многочлены	20	10	10
8.	Матрицы и определители.	24	12	12
9.	Векторные пространства.	28	14	14
10.	Системы уравнений.	12	6	6
11.	Линейные отображения.	24	12	12
12.	Полиномиальные матрицы.	24	12	12
13.	Квадратичные формы.	20	10	10
14.	Евклидовы и унитарные пространства.	20	10	10
15.	Изометрические и симметрические преобразования	8	4	4
16.	Векторные и матричные нормы. Псевдообратная матрица	8	4	4
	Раздел 3. Прикладная алгебра			
17.	Решение сравнений в кольце целых чисел.	12	6	6
18.	Группы и их гомоморфизмы.	12	6	6
19.	Кольца и их гомоморфизмы.	8	4	4
20.	Конечные поля и многочлены над ними.	12	6	6
21.	Пороговая схема. Алгоритмы шифрования. RSA-криптосистемы	12	6	6
22.	Матричные коды.	12	6	6
	Всего	340	170	170

Содержание

Введение

Предмет дисциплины «Геометрия и алгебра». Исторические сведения о развитии этого раздела математики. Роль и место геометрии и алгебры в системе математического образования.

Раздел 1. Аналитическая геометрия на плоскости и в пространстве

1. Системы координат на прямой, плоскости и пространстве

Метод координат на прямой, плоскости и в пространстве. Прямоугольная, полярная, цилиндрическая и сферическая системы координат.

2. Векторы

Понятие вектора. Линейные операции над векторами. Скалярное, векторное и смешанное произведение векторов.

3. Прямые и плоскости

Различные виды уравнений прямой на плоскости и в пространстве. Уравнения плоскости. Взаимное расположение прямых и плоскостей.

4. Фигуры второго порядка на плоскости и в пространстве

Фигуры второго порядка на плоскости и в пространстве. Приведение уравнений линий и поверхностей второй порядка к каноническому виду.

Раздел 2. Алгебра

5. Алгебраическая операция. Группа, кольцо, поле

Бинарное отношение. Отношения эквивалентности и порядка, классы эквивалентности. Алгебраическая операция. Группа. Кольцо. Поле. Изоморфизмы полей.

6. Комплексные числа

Поле комплексных чисел. Алгебраическая, тригонометрическая и экспоненциальная формы комплексных чисел. Возведение в степень и извлечение корня n-ой степени из комплексного числа. Корни из единицы.

7. Многочлены

Кольцо многочленов над полем. Деление с остатком. Алгоритм Евклида. Корни многочлена. Разложение многочленов на неприводимые многочлены. Интерполяция. Схема Горнера. Рациональные дроби. Многочлены над Q. Неприводимые многочлены над Q. Критерий Эйзенштейна.

8. Матрицы и определители

Матричная алгебра. Определители. Теорема Лапласа. Обратная матрица. Системы линейных уравнений. Правило Крамера. Метод Гаусса. Матричные уравнения.

9. Векторные пространства

Векторное (линейное) пространство. Линейная зависимость и независимость векторов. Базис и размерность. Подпространства. Линейные оболочки. Сумма и

пересечение подпространств. Ранг системы векторов. Ранг матрицы и теорема о базисном миноре.

10.Системы уравнений

Критерий совместности систем линейных уравнений. Общее решение систем линейных уравнений.

11. Линейные отображения

Линейные отображения. Изоморфизм векторных пространств. Ядро и образ линейного преобразования (оператора). Невырожденное линейное преобразование. Собственные векторы и собственные значения. Характеристическая матрица и характеристический многочлен. Операторы простой структуры.

12. Полиномиальные матрицы

Полиномиальные матрицы. Критерии эквивалентности полиномиальных матриц. Критерий подобия матриц. Минимальный многочлен. Теорема Гамильтона-Кели. Нормальные формы матриц: жорданова нормальная форма матрицы, обобщенная жорданова форма матрицы, нормальные формы Фробениуса.

13. Квадратичные формы

Билинейные и квадратичные формы. Метод Лагранжа приведения квадратичной формы к каноническому виду. Критерии эквивалентности квадратичных форм над полем R и над полем C. Приведение квадратичной формы к каноническому виду при помощи ортогональных преобразований. Критерии знакоопределённости действительных квадратичных форм. Эрмитовы формы.

14. Евклидовы и унитарные пространства

Евклидовы и унитарные пространства. Процесс ортогонализации Грама-Шмидта.

15. Изометрические и симметрические преобразования

Изометрический оператор. Самосопряжённый оператор. Разложение произвольного линейного оператора в произведение изометрического и самосопряжённого операторов.

16. Векторные и матричные нормы. Псевдообратная матрица

Векторные и матричные нормы. Эквивалентность норм. Псевдообратная матрица Мура-Пенроуза. Нормальное псевдорешение системы линейных уравнений.

Раздел 3. Прикладная алгебра

17. Решение сравнений в кольце целых чисел

Кольцо целых чисел, НОК, НОД. Алгоритм Евклида. Взаимно простые числа, простые числа, факторизация. Сравнения первой степени, системы сравнений первой степени, функция Эйлера, теорема Эйлера. Первообразные корни и индексы.

18. Группы и их гомоморфизмы

Нормальные подгруппы и факторгруппы. Гомоморфизмы групп. Циклические группы. Основы теории абелевых групп. Действие группы на множестве. Орбиты и стабилизаторы точек. Действие группы на смежных классах по подгруппе.

19. Кольца и их гомоморфизмы

Гомоморфизмы и идеалы колец. Факторкольца. Разложение колец в прямую сумму неразложимых идеалов.

20. Конечные поля и многочлены над ними

Поля и их характеристики. Алгебраические расширения полей. Поле разложения. Строение конечных полей. Многочлены над конечными полями. Порядок многочлена и примитивные многочлены.

21. Пороговая схема. Алгоритмы шифрования. RSA-криптосистема

Пороговая схема на основе CRT. Распределение ключей по Диффи-Хелмену. Структура алгоритмов DES, ГОСТ, IDEA. Структура обратных преобразований, роль инволюций. RSA-криптосистема и система цифровой подписи на её основе.

22. Матричные коды

Групповые коды. Матричные коды. Расстояние Хемминга. Кодирующая и проверочная матрицы. Лидеры и синдромы смежных классов. Коды Хемминга. Полиномиальные коды, линейные рекурренты. Максимальный период. Регистры сдвига с прямой и обратной связью.

Литература

Основная

1. Биркгоф Г., Барти Т. Современная прикладная алгебра. М., 2005г., 400с.
2. Бурдун А.А., Мурашко Е.А., Толкачев М.М., Феденко А.С. Сборник задач по алгебре и аналитической геометрии. – Мн., “Университетское”, 1989, 222с
3. Ильин В.А., Позняк Э.Г. Аналитическая геометрия. – М.: “Наука”, 1974г., 232с.
4. Ильин В.А., Позняк Э.Г. Линейная алгебра. – М: “Наука”, 1981г., 294с
5. Лидл Р., Нидерайтер Р. Конечные поля. М., 1989г., 428с
6. Милованов М.В., Тышкевич Р.И., Феденко А.С. Линейная алгебра и аналитическая геометрия. I. – Мн., “Выш. школа”, 1976г., 544с.
7. Милованов М.В., Тышкевич Р.И., Феденко А.С. Линейная алгебра и аналитическая геометрия. II. – Мн., “Выш. школа”, 1984г., 302с.
8. Размыслович Г.П., Феденя М.М., Ширяев В.М. Геометрия и алгебра. – Мн., “Университетское”, 1987г., 350с.
9. Размыслович Г.П., Феденя М.М., Ширяев В.М. Сборник задач по геометрии и алгебре. – Мн., ”Университетское”, 1999г., 384с
10. Тышкевич Р.И., Феденко А.С. Линейная алгебра и аналитическая геометрия. Мн., “Выш. школа”, 1976г., 544с.
11. Харин Ю.С. Математические и компьютерные способы криптографии. Мн., 2003г., 391с.
12. Шнеперман Л.Б. Курс алгебры и теории чисел в задачах и упражнениях. Т1., Мн: Вышэйшая школа, 1986, 272с.
13. Шнеперман Л.Б. Курс алгебры и теории чисел в задачах и упражнениях. Т2., Мн: Вышэйшая школа, 1987, 256с.

Дополнительная

1. Беклемишев Д.В. Курс аналитической геометрии и линейной алгебры. М.: “Наука”, 1984г., 320с.
2. Брассар Т. Современная криптология. М.: Полимед, 1999г., 385с.
3. Воеводин В.В. Линейная алгебра. – М., “Наука”, 1990, 400с.
4. Гантмахер Ф.Р. Теория матриц. М.: “Наука”, 1967г., 575с.
5. Клетеник Д.В. Сборник задач по аналитической геометрии. – М.: “Наука”, 1980, 240с.
6. Курош А.Г. Курс высшей алгебры. – М., “Наука”, 1975, 431с.
7. Кострикин А.И., Манин Ю.И. Линейная алгебра и геометрия. М.: “Наука”, 1986г., 304с.
8. Проскуряков И.В. Сборник задач по линейной алгебре. М.: “Наука”, 1978г., 384с.
9. Фаддеев Д.Н., Соминский И.С. Сборник задач по высшей алгебре. – М.: “Наука”, 1977, 188с.
10. Ященко В.В. Введение в криптографию. М., МЦНМО, 2001г., 287с.