

**Вопросы к экзамену по курсу «Алгебра и геометрия»  
(ФИТ, 1 семестр 2016/17 уч. года)**

1. Геометрические векторы: определение, операции сложения векторов и умножения вектора на вещественное число, свойства операций.
2. Линейные комбинации геометрических векторов, линейная зависимость и независимость, базис и единственность разложение вектора по базису, преобразование координат при сложении векторов и умножении на число.
3. Декартова система координат: координаты точки и вектора, заданного двумя точками, деление отрезка в данном отношении.
4. Скалярное произведение геометрических векторов: определение и основные свойства, скалярное произведение линейных комбинаций, формула скалярного произведения в координатах в ортонормированном базисе, выражение длины вектора и угла между ненулевыми векторами через скалярное произведение, формулы ортогональной проекции вектора на направление ненулевого вектора и разложения вектора по ортогональному базису.
5. Векторное произведение геометрических векторов: определение, основные свойства, векторное произведение линейных комбинаций, формула векторного произведения в правом ортонормированном базисе, ориентированная площадь параллелограмма на плоскости и определитель второго порядка.
6. Смешанное произведение геометрических векторов: определение, основные свойства, связь с ориентируемым объемом параллелепипеда и выражение через координаты в правом ортонормированном базисе в виде определителя третьего порядка.
7. Дополнительные свойства векторного произведения: двойное векторное произведение, тождество Якоби, скалярное произведение двух векторных произведений, формула косинусов сферической геометрии, векторное произведение и формулы Крамера.
8. Преобразование координат вектора и точки при замене базиса и декартовой системы координат, вид параллельных переносов, отражений и поворотов плоскости в координатах в подходящей декартовой системе координат.
9. Уравнения прямой на плоскости: общее, нормальное, в отрезках координатных осей, параметрические, каноническое, по двум точкам, через определитель.
10. Уравнения плоскости в пространстве: общее, нормальное, в отрезках координатных осей, параметрические, каноническое, по трем точкам, через определитель.
11. Уравнения прямой в пространстве: задание системой двух линейных уравнений, параметрические уравнения, каноническое, по двум точкам.
12. Формулы расстояний между двумя точками, от точки до прямой на плоскости, от точки до плоскости в пространстве, от точки до прямой в пространстве, между параллельными и скрещивающимися прямыми в пространстве.

13. Вычисление углов между двумя ненулевыми векторами, между прямыми на плоскости, между плоскостями в пространстве, между прямой и плоскостью в пространстве.
14. Эллипс: каноническое уравнение, свойства симметрии и характеристики, фокальное, директориальное и оптическое свойства.
15. Гипербола: каноническое уравнение, свойства симметрии и характеристики, фокальное, директориальное и оптическое свойства.
16. Парабола: каноническое уравнение, свойства симметрии и характеристики, фокально-директориальное и оптическое свойства.
17. Приведение общего уравнения кривой второго порядка на плоскости к каноническому виду — вывод уравнений центров симметрии.
18. Приведение общего уравнения кривой второго порядка на плоскости к каноническому виду — центральный случай.
19. Приведение общего уравнения кривой второго порядка на плоскости к каноническому виду — нецентральный случай.
20. Эллипсоид: каноническое уравнение, свойства симметрии и характеристики, теорема о круговых сечениях.
21. Конус: каноническое уравнение, свойства симметрии, теорема о плоских сечениях кругового конуса (шары Данделена).
22. Однополостный и двуполостный гиперboloиды: каноническое уравнение, свойства симметрии, теорема о прямолинейных образующих.
23. Эллиптический и гиперболический параболоиды: каноническое уравнение, свойства симметрии, теорема о прямолинейных образующих.
24. Классификация и вид цилиндрических поверхностей.
25. Алгебраические операции, алгебраические структуры, изоморфизм.
26. Абелевы группы, кольца, поля: аксиоматика, простейшие следствия аксиом, примеры, кольца вычетов (без доказательства), делители нуля и характеристика поля.
27. Векторные пространства: аксиоматика, примеры, простейшие следствия аксиом, базисы и теорема об изоморфизме координатным пространствам над полем.
28. Алгебры: аксиоматика, примеры, теорема о задании алгебр произведениями базисных элементов, поле комплексных чисел.
29. Алгебра матриц.
30. Системы линейных уравнений и метод Гаусса: приведение матриц к ступенчатому и разрешенному виду, критерий совместности и общее решение совместной системы линейных уравнений, однородные системы и фундаментальные системы решений.

31. Теорема о размерности векторного пространства.
32. Подпространства: линейная оболочка и ранг системы векторов, теорема о размерности и базисе подпространства конечномерного пространства.
33. Сумма и пересечение подпространств: определение и теорема о размерности суммы; прямые суммы: определение и критерий на языке пересечений.
34. Перестановки: определение, инверсии и четность, теорема о количестве и поведении при транспозициях.
35. Определитель матрицы как функция системы ее строк, теорема о существовании и единственности.
36. Дополнительные свойства определителя: поведение при элементарных преобразованиях системы строк, определитель треугольной матрицы, транспонированной матрицы, полураспавшейся матрицы, произведения матриц.
37. Теорема о разложении определителя по строке (столбцу), формула для обратной матрицы, формулы Крамера в общем случае.
38. Теорема о ранге для матриц.
39. Кольцо целых чисел: теорема о делении с остатком.
40. Наибольший общий делитель и алгоритм Евклида.
41. Критерий разрешимости линейного диофантова уравнения и алгоритм поиска частного решения.
42. Свойства взаимно простых чисел.
43. Общее решение линейного диофантова уравнения.
44. Основная теорема арифметики.
45. Конструкция кольца вычетов по модулю  $n$ , критерий обратимости числа по модулю  $n$ , поле вычетов.
46. Китайская теорема об остатках (древняя и современная формы), сведение к примарному модулю.
47. Представление арифметики чисел порядка  $10^{90}$  в 64-х разрядной бинарной арифметике.
48. Группа обратимых элементов кольца вычетов по модулю  $n$ : определение и вычисление  $\varphi$ -функции Эйлера, теорема об общем периоде элементов конечной абелевой группы, малая теорема Ферма и ее обобщение — формула Эйлера.
49. Порядок элемента группы и три леммы о порядках элементов.

50. Определение циклической группы и теорема о конечных подгруппах мультипликативной группы поля.
51. Определение дискретного логарифма и описание *RSA*-криптографии с открытым ключом.
52. Группы подстановок: определение, правило умножения и теорема о групповой структуре, знак подстановки и его мультипликативность, разложение на циклы и транспозиции, знак и количество транспозиций в разложении.
53. Определение символа Якоби (по Золотареву), его свойства: мультипликативность, критерий разрешимости квадратичного уравнения по простому модулю, вычисление символа  $\left(\frac{-1}{n}\right)$ , лемма 1 и вычисление символа  $\left(\frac{2}{n}\right)$ .
54. Определение символа Якоби (по Золотареву), его свойства: периодичность — леммы 2 и 3, закон взаимности Гаусса–Якоби.