

Эллиптические кривые и криптография.

Программа курса.

Осенний семестр 2011/2012 учебного года

- (1) Простые поля. Характеристика поля. Строение конечных полей. Мультипликативная группа конечного поля. Неприводимые многочлены над конечными полями.
- (2) Отображение Фробениуса. Алгебраическое замыкание конечного поля. Совершенные поля. Алгебраическое расширение совершенного поля совершенно. Сепарабельные расширения.
- (3) Трансцендентные расширения. Алгебраическая зависимость. Базисы трансцендентности. Лемма об алгебраической зависимости. Число элементов базиса трансцендентности не зависит от выбора базиса.
- (4) Аффинное пространство. Алгебраические множества. Топология Зарисского. Аффинные многообразия. Связь с простыми идеалами. Примеры. Лемма о двух многочленах. Простые идеалы в $\mathbb{k}[x, y]$.
- (5) Кольцо регулярных функций. Поле рациональных функций. Регулярность функции в точке. Локальное кольцо точки. Размерность. Примеры. Размерность вложенных многообразий. Примеры. Размерность гиперповерхности.
- (6) Касательное пространство Зарисского. Особые и неособые точки. Примеры. Множество особенностей. Кратность пересечения прямой и гиперповерхности. Множество особых точек – алгебраическое собственное подмножество.
- (7) Проективные алгебраические множества. Топология Зарисского. Неприводимость. Градуированные кольца. Однородные идеалы. Однородное координатное кольцо. Примеры. Аффинное покрытие.
- (8) Теорема Безу. Точки перегиба. Гессиан. Эллиптические кривые. Существование точек перегиба.
- (9) Нормальная форма Вейерштрасса. Дискриминант и j -инвариант. Эллиптические кривые, определенные над алгебраически незамкнутым полем.
- (10) Точки перегиба кубических кривых и конечные геометрии. Автоморфизмы конфигураций точек перегиба. Эллиптическая кривая определяется своим j -инвариантом.
- (11) Групповой закон на эллиптической кривой. Упрощенный групповой закон. Лемма о кубических кривых. Доказательство ассоциативности (для общих точек).
- (12) Явные формулы для группового закона. Эллиптические кривые над незамкнутыми полями. Точки порядка 2 и 3.
- (13) Римановы поверхности. Эллиптические функции. Теоремы Лиувилля. Функция Вейерштрасса. Ее свойства.
- (14) Поле эллиптических функций. Дифференциальное уравнение для функции Вейерштрасса. Групповой закон и эллиптические функции.