Эллиптические кривые и криптография.

Программа курса.

Осенний семестр 2010/2011 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. Неприводимые многообразия. Связь с простыми идеалами. Примеры. Лемма о двух многочленах. Алгебраические подмножества аффинной плоскости. Разложение на неприводимые компоненты (без доказательства). Простые идеалы в $\Bbbk[x, y]$.

(5) Разложение на неприводимые компоненты (случай поднмогообразий $\mathbb{A}^2$). Кольцо регулярных функций. Поле рациональных функций. Регулярность функции в точке. Размерность. Примеры.

(6) Размерность вложенных многообразий. Примеры. Размерность гиперповерхности. Локальное кольцо точки. Его максимальный идеал.

(7) Касательное пространство Зарисского. Особые и неособые точки. Примеры. Множество особенностей. Кратность пересечения прямой и гиперповерхности. Геометрическая интерпретация касательного пространства.

(8) Проективные алгебраические множества. Топология Зарисского. Неприводимость. Градуированные кольца. Однородное координатное кольцо. Поле рациональных функций. Размерность. Примеры. Аффинное покрытие. Неособость.

(9) Теорема Безу. Точки перегиба. Гессиан. Эллиптические кривые. Существование точек перегиба.

(10) Нормальная форма Вейерштрасса. Дискриминант и j-инвариант. Эллиптические кривые, определенные над алгебраически незамкнутым полем.

(11) Точки перегиба кубических кривых и конечные геометрии. Автоморфизмы конфигураций точек перегиба. Эллиптическая кривая определяется своим j-инвариантом.

(12) Групповой закон на эллиптической кривой. Упрощенный групповой закон. Лемма о кубических кривых. Доказательство ассоциативности (для общих точек).

(13) Явные формулы для группового закона. Эллиптические кривые над незамкнутыми полями. Точки порядка 2 и 3.

(14) Понятие римановой поверхности. Комплексные торы. Эллиптические функции. Теоремы Лиувилля. Функция Вейерштрасса. Ее свойства.

(15) Поле эллиптических функций. Дифференциальное уравнение для функции Вейерштрасса. Групповой закон и эллиптические функции.

(16) Рациональные кривые. Примеры. Нерациональность эллиптических кривых.