Семинар 16 (кое-что про конечные поля)

Наше Верую: у каждого поля K есть алгебраическое замыкание $\bar{K}$, определенное с точностью до изоморфизма, тождественного на K (доказательство можно прочесть, например, в классическом учебнике Ван дер Вардена "Алгебра").

В дальнейшем F_q обозначает конечное поле из q элементов, $q = p^n, p$ простое, F_p – базовое поле характеристики p.

Во всех задачах требуется доказать сформулированные в них утверждения. Все утверждения касаются конечных подполей поля $\bar{F}_p$ и их расширений.

1. Пусть V – векторное пространство размерности l над полем F_q. Тогда $|V| = q^l$.

2. Пусть E – конечное расширение поля F_q степени e. Тогда $|E| = q^e$.

3. Пусть $F_q = [u \in \bar{F}_p | u^q - u = 0]$. Тогда F_q – конечное расширение степени n.

4. Расширение, построенное в задаче 3, является полем раложения (какого многочлена?) над полем F_p. Это единственное поле в $\bar{F}_p$, в котором $q = p^n$ элементов.

5. Конечное поле F_q является простым расширением поля F_p.

6. Подполя поля F_q находятся во взаимно-однозначном сответствии с делителями числа n.

7. $\bar{F}_p = \bigcup F_{p^n}$ (объединение по всем натуральным n).

8. Пусть $f(x)$ неприводимый многочлен степени k над полем F_p. Многочлен $f(x)$ тогда и только тогда делит многочлен $x^q - x$, когда $k|n$.

9. В конечном расширении поля F_2 любой элемент является квадратом.

10. Сколько квадратов в поле F_{81}? А сколько в этом поле седьмых степеней?