Семинар 19

Конечные поля

0. Дано-коммутативное кольцо с единицей, без делителей нуля. Доказать, что любая конечная подгруппа мультипликативной группы обратимых элементов кольца является циклической.

1. Сколько существует неприводимых многочленов второй степени над конечным полем из пяти элементов?

2. $\mathbb{F}_{p^m} < \mathbb{F}_{p^n} \iff m|n$. Доказать.

3. Пусть p – нечетное простое число. Многочлен X^2+1 тогда и только тогда неприводим над полем $\mathbb{F}_p$, когда $p \equiv 3 \mod 4$.

4. Докажите, что расширение $\mathbb{F}_{p^{md}}|\mathbb{F}_{p^m}$ является простым.

5. Докажите, что группа $\mathrm{Gal}(\mathbb{F}_{p^{md}}|\mathbb{F}_{p^m})$ порождается автоморфизмом Фробениуса $\Phi_{p^d} : \bar{\mathbb{F}}_p \to \bar{\mathbb{F}}_p$, $\Phi_{p^d}(\alpha) = \alpha^{p^d}$.

6. Пусть γ – образующая мультипликативной группы поля $\mathbb{F}_{p^m}$. Докажите, что степень γ над полем $\mathbb{F}_p$ равна m.