
Below we use the following notation:
Txbk – "Codinig theory and Cryptography" by Hankerson & others.

We may also use notations:
♢ – the proof is not obligatory,
⧫ – an important topic, the proof in particular.
Th - Theorem, Pr - Proposition, Lm - Lemma.

Content of lectures 9-10.

Lecture 9.

Characteristic of a field.
Th: a finite field F has p^n elements, where $p = charF$ and $n = dim(F/\mathbb{Z}_p)$.
⧫ Any irreducible polynomial of degree n over $\mathbb{Z}_p$ divides $x^m - 1$,
where $m = p^n - 1$.
All finite field of given number of elements are isomorphic.
†Txbk: Related things are in 5.2.
‡. In [Pless] you can consult ch.4.

Lecture 10.

Cyclotimic sets.
Three ways to organize the parity checking for a cyclic code:

- a) calculating a remainder,
- b) using a parity check polynomial,
- c) using a parity check matrix with elements in the extension field.

Vandermonde determinants: an introduction.
†Txbk: 4.3, 4.5.
‡[Pless]: 5.3, 7.1, 7.2.