
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 7-8.

Lecture 7.

♦ Th: any ideal in $R = F[x]/(x^n - 1)$ is principal.
The generating polynomial for a cyclic code.
The dimension of the cyclic code given by its generating polynomial.
Two ways to construct an encoding map for a cyclic code
given by its generating polynomial.
Slogan: "Irredicible monic polynomials ↔ orbits of a Galois group".
Explaining it with the example: irreducible polynomials over $\mathbb{R}$
(we proved that there is no irreducible polynomials of degree larger than 2).
†It seems Txbk does not mention ideals and generating polynomials
are there in 4.3.
‡. [Pless] has a short section 5.2 on these matters.

Lecture 8.

Automorphisms of a field. Examples: $\mathbb{C}$, $\mathbb{F}_9$, $\mathbb{F}_8$.
Frobenious automorphism of a finite field.
The ground field (in respect to an automorphism).
The subfield of "sums of 1" – prime subfield.
♦ Finding all the automorphisms of $\mathbb{F}_8$.
†The topic is related to Txbk 5.2, but more Galois theory is included.
‡Same, related to [Pless]: 4.2-4.4, but quite different in presentation.