Finite field isomorphisms

Given a prime p and a positive integer n we know there is, up to isomorphism, only one field of cardinality p^n. However, the common proof of this theorem is not constructive and does not provide an isomorphism if two finite fields of the same cardinality are presented.

Only in 1991, Lenstra proved there exists a deterministic polynomial algorithm that given two extensions of finite fields of the same degree computes an isomorphism between them, making use of cyclotomic ring extensions.

In this lecture I will first discuss some special cases and then I will give a sketch of Lenstra's proof.