Excercise 1. *(a) Find an irreducible polynomial f of degree 2 in $\mathbf{F}_3[x]$. Then $\mathbf{F}_9 = \mathbf{F}_3[x]/(f)$.*
(b) Which elements of $\mathbf{F}_9$ are generators of its multiplicative group $\mathbf{F}_9^*$?
(c) Which elements of $\mathbf{F}_9$ have square roots in $\mathbf{F}_9$?
(d) Prove that the product of all elements of $\mathbf{F}_9^*$ is 2.
(e) Show that the additive group of $\mathbf{F}_9$ is not cyclic.

Sol.: (a) The field $\mathbf{F}_9$ is a quadratic extension of $\mathbf{F}_3$: we obtain it by adding a root ζ of a degree 2 irreducible monic polynomial in $\mathbf{F}_3[x]$. For example x^2+1, or x^2+x+2, or x^2+2x+2.
Let's use x^2+2x+2. Then $\mathbf{F}_9 \cong \mathbf{F}_3[x]/(x^2+2x+2)$. Using the isomorphism $\mathbf{F}_9 \cong \mathbf{F}_3[x]/(x^2+2x+2)$, we can represent the elements of $\mathbf{F}_9$ as polynomials of degree ≤ 2 with coefficients in $\mathbf{F}_3$, where the product is computed modulo the relation $x^2 = -2x-2 = x+1$.

(b) $\mathbf{F}_9^*$ is a cyclic group of 8 elements: $1, 2, x, 2x, 1+x, 2+x, 1+2x, 2+2x$. It contains $\varphi(8) = 4$ generators, that is elements of order 8.

For example, let's check that x is a generator: the powers of x modulo $x^2 = x+1$ exhaust all $\mathbf{F}_9^*$.

$$x, \quad x^2 = x+1, \quad x^3 = x(x+1) = 2x+1, \quad x^4 = x(2x+1) = 2,$$

$$x^5 = 2x, \quad x^6 = 2x^2 = 2x+2, \quad x^7 = x(2x+2) = x+2, \quad x^8 = x(x+2) = 1.$$

The other three generators of $\mathbf{F}_9^*$ are x^k, with $gcd(k,8) = 1$, namely

$$x^3 = 2x+1, \quad x^5 = 2x, \quad x^7 = x+2.$$

(c) The elements of $\mathbf{F}_9$ which have a square root in $\mathbf{F}_9$ are precisely 0 and the squares in $\mathbf{F}_9^*$, in other words, the even powers of a generator:

$$x^2 = x+1, \quad x^4 = 2, \quad x^6 = 2x+2, \quad x^8 = 1.$$

(d) In $\mathbf{F}_9^*$ every element z is paired with its inverse $z^{-1} \neq z$, except for 1 and the unique element of order 2 (there is one because the cardinality of $\mathbf{F}_9^*$ is even!). As a result,

$$\prod_{z \in \mathbf{F}_9^*} z = 1 \cdot 2 = 2.$$

(in general, for every prime p one has $\prod_{z \in \mathbf{F}_{p^m}^*} z = 1 \cdot (-1) = -1$ (see Wilson's theorem))

(e) As an additive group, $\mathbf{F}_9$ is isomorphic to $\mathbf{Z}_3 \times \mathbf{Z}_3$, which is not cyclic: every element different from the neutral element in $\mathbf{Z}_3 \times \mathbf{Z}_3$ has order 3.

Excercise 2. *Draw the Hasse diagrams of the subfields of each $\mathbf{F}_{2^k}$ for $k = 1, .., 6$..*

Sol.: There is a field inclusion $\mathbf{F}_{2^h} \hookrightarrow \mathbf{F}_{2^k}$ if and only if $h \mid k$.
$k = 1$:

$$\mathbf{F}_2$$

$k = 2$:

$$\mathbf{F}_2 \hookrightarrow \mathbf{F}_{2^2}$$

$k = 3$:

$$\mathbf{F}_2 \hookrightarrow \mathbf{F}_{2^3}$$

$k = 4$:

$$\mathbf{F}_2 \hookrightarrow \mathbf{F}_{2^2} \hookrightarrow \mathbf{F}_{2^4}$$

$k = 5$:

$$\mathbf{F}_2 \hookrightarrow \mathbf{F}_{2^5}$$

$k = 6$: