7.9 The arithmetical representation of $GF(9)$

Example 7.5.2, Remark 7.5.3, Example 7.2.2, Example 7.7.7 submirize the computational approach allowing to produce an arthmetical model for a Galois field of characteristic 2.

We discuss here an arithmetical model for a finite field $F, \mathrm{char}(F) \neq 2$, using as example the easy, but not trivial, case of $GF(9)$.

For $n = 9 = 3^2$ we have $n - 1 = 8 = 2^3$ so that

$$g_8(X) := X^8 - 1 \in \mathbb{Z}_3[X]$$

factorizies as

$$g_8 = \Phi_1 \Phi_2 \Phi_4 \Phi_8$$

where the four factors are the cyclotomic polynomials over $\mathbb{Z}_3$ which have the values

$$\begin{array}{lclcl} \Phi_1 & := & & & X - 1, \\ \Phi_2 & := & \frac{\Phi_1(X^2)}{\Phi_1(X)} & = & X + 1, \\ \Phi_4 & := & \Phi_2(X^2) & = & X^2 + 1, \\ \Phi_8 & := & \Phi_4(X^2) & = & X^4 + 1. \end{array}$$

According to Theorem 7.2.2, $X^9 - X \in \mathbb{Z}_3[X]$ factorizes into the 3 trivial linear factors $X, \Phi_1 = X - 1$ and $\Phi_2 = X + 1$ and into all irreducible polynomials of degree 2 over $\mathbb{Z}_3$; an obvious degree count allows to deduce that they are $\frac{9-3}{2} = 3$ and it is sufficient to list all 9 polynomials

$$h(X) := X^2 + aX + b, a, b \in \mathbb{Z}_3 = \{-1, 0, 1\}$$

and preserve those which satisfy $h(-1)h(0)h(1) \neq 0$ in order to obtain the required 3 irreducible factors of degree 2 of $\frac{X^8-1}{X^2-1}$, namely:

$$X^2 + X - 1, \quad X^2 - X - 1 \text{ and } X^2 + 1 = \Phi_4.$$

Of course we have

$$\Phi_8 = X^4 + 1 = (X^2 + X - 1) \cdot (X^2 - X - 1)$$

as it is easy to verify.

Remark that each root ξ of a factor of $\Phi_4 = X^2 + 1$ is not a primitive element of $GF(9)$ since $\xi^4 = 1$; in fact they satisfy $\xi^2 = -1$ and, hence, $\xi^4 = 1$.

In order to obtain a primitive element we thus select a factor of Φ_8, *e.g.* $f := X^2 + X - 1$ so that any root ξ of f satisfies the relation $\xi^2 = -\xi + 1$. Thus a recursive application of the formula

$$r_i(X) = \mathbf{Rem}(Xr_{i-1}, f) \in \mathbb{Z}_3(X)/f$$

using the seed $r(1) = X$, gives us the logarithmic table of $GF(3^2)$ reported in Tab. 7.1 whose correspinding Zech table is reported in Tab. 7.2

Table 7.1. Logarithm table for $GF(9)$

i	r(i)	i	r(i)
1	ξ	5	$-\xi$
2	$-\xi+1$	6	$\xi-1$
3	$-\xi-1$	7	$\xi+1$
4	-1	8	1

Table 7.2. Zech table for $GF(9)$

i	Z(i)	i	Z(i)
1	7	0	4
2	3	7	6
3	5	6	1
4	$\star$	5	2

To complete our analysis we need to associate the four cycles $\{i, 3i\}$ of the permutation $\pi_3 : \mathbb{Z}_8 \to \mathbb{Z}_8$ with the corresponding irreducible factors of g_8, which can be obtained by computing $(X - \xi^i)(X - \xi^{3i})$; we obtain:

$\{1,3\}$	X^2+X-1
$\{2,6\}$	X^2+1
$\{4\}$	$X+1$
$\{5,7\}$	X^2-X-1
$\{0\}$	$X-1$

However, the relation can be directly deduced by an easy argument:

- The cycle $\{1,3\}$ of course is related to the minimal polynomial f of ξ.
- Remarking that the other factor $g = X^2 - X - 1$ of Φ_8 satisfies the relation

  $$X^2 g(\frac{1}{X}) = -f(X)$$

  so that

  $$f(\theta) = 0 \iff f(\theta^{-1}) = 0$$

  and that for each $\theta = \xi^i$ we have $\theta^{-1} = \xi^{8-i}$, the cycle associated to $g = X^2 - X - 1$ is $8 - \{1,3\} = \{5,7\}$.
- Finally $\theta = \xi^2$ necessarily satisfy $\theta^4 = \xi^8 = 1$ so it is a root of Φ_4.