7.9 The arithmetical representation of GF(9)

Example 7.5.2, Remark 7.5.3, Example 7.2.2, Example 7.7.3 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

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

factorizes as

$$g_8 = \varphi_1\varphi_2\varphi_4\varphi_8$$

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

$$\begin{aligned} \varphi_1 &:= & & X - 1, \\ \varphi_2 &:= \frac{\varphi_1(X^2)}{\varphi_1(X)} &=& X + 1, \\ \varphi_4 &:= \varphi_2(X^2) &=& X^2 + 1, \\ \varphi_8 &:= \varphi_4(X^2) &=& X^4 + 1. \end{aligned}$$

According to Theorem 7.2.2, $X^9 - X \in \mathbb{Z}_3[X]$ factorizes into the 3 trivial linear factors X, $\varphi_1 = X - 1$ and $\varphi_2 = X + 1$ 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:

$$X^2 + X - 1, \quad X^2 - X + 1 \text{ and } X^2 + 1 = \varphi_4.$$

Of course we have

$$\varphi_8 = X^4 + 1 = (X^2 + X - 1)\cdot(X^2 - X + 1)$$

as it is easy to verify.

Remark that each root ξ of a factor of $\varphi_4 = X^2 + 1$ 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

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

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	»	5	¡»
2	¡» + 1	6	» ¡ 1
3	¡» ¡ 1	7	» + 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	?	5	2

To complete our analysis we need to associate the four cycles fi;3ig of the permutation $_3$: Z_8 ! Z_8 with the corresponding irreducible factors of g_8, which can be obtained by computing (X ¡ »^{i})(X ¡ »^{3i}); we obtain:

f1;3g	X^2 + X ¡ 1
f2;6g	X^2 + 1
f4g	X + 1
f5;7g	X^2 ¡ X + 1
f0g	X ¡ 1

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

† The cycle f1;3g of course is related to the minimal polynomial f of ».
† Remarking that the other factor g = X^2 ¡ X + 1 of '$_8$ satisfies the relation

$$X^2 g(\frac{1}{X}) = ¡ f(X)$$

so that

f( ) = 0 ( ) f($^{¡1}$) = 0

and that for each = »^{i} we have $^{¡1}$ = »$^{8¡i}$, the cycle associated to g = X^2 ¡ X + 1 is 8 ¡ f1;3g = f5;7g.
† Finally = »^{2} necessarily satisfy ^{4} = »^{8} = 1 so it is a root of '$_4$.