

Let  $\alpha$  be a root of the polynomial  $p(X) = X^6 + X + 1$  over  $Z_2$  and let  $M$  be the ring of polynomial expressions in  $\alpha$  over  $Z_2$ . To prove in a simple way that  $M$  is a field (of order 64) we have to show that  $p(X)$  is irreducible (over  $Z_2$ ). The only possible divisors we have to exclude belong to the set  $S$  of irreducible polynomials of degree at most 3, where  $S = \{X, X+1, X^2+X+1, X^3+X+1, X^3+X^2+1\}$ . Suppose for instance that  $X^3+X+1$  divides  $p(X)$ , then for any root  $a$  of  $X^3+X+1$  both  $a^3+a+1=0$  and  $a^6+a+1=0$ , which leads to  $a^3 \in \{0, 1\}$  and a contradiction follows. Similarly for the other cases. We claim that  $\alpha$  is in fact a primitive element of  $M$ , that is, it is a generator of the multiplicative group  $M^* = M \setminus \{0\}$ , of order 63. Suppose not. Then either  $\alpha^{21} = 1$  or  $\alpha^9 = 1$ , for 21 and 9 are the two maximal proper divisors of 63. Combining the first assumption with  $\alpha^6 + \alpha + 1 = 0$  leads to  $\alpha^3 = \alpha^{24} = (\alpha + 1)^4 = \alpha^4 + 1$ , an equation for  $\alpha$  of degree less than the degree 6 of  $p(X)$ , whereas, by its irreducibility,  $p(X)$  is the minimal polynomial of  $\alpha$  (over  $Z_2$ ). The second case is similar. [There are, of course, large tables of irreducible and primitive polynomials available on the internet or Maple may be used]

```
> restart: p(X):=X^6+X+1: alias(alpha=RootOf(p(X))):
beta:=alpha^21: delta:=alpha^9:
f:=x->x^2 mod 2:fmap:=x->map(f,x):
F:=x->2*x mod 63:
```

```
> Irreduc(p(X)) mod 2:Primitive(p(X)) mod 2:%,%%;
true, true
```

```
> Factor(p(X)) mod 2: Factor(p(X),alpha) mod 2:
print("over {0,1}",'p(X)'=%%, "over M", 'p(X)'=%);
"over {0,1}", p(X) = X^6 + X + 1, "over M", p(X) = (X + alpha^4 + alpha + 1) (X + alpha) (X + alpha^3 + alpha^2) (X + alpha^3 + 1) (X + alpha^4) (X + alpha^2)
```

We take  $s = \{\alpha^k, k = 0 \dots 5\}$  as (standard) basis of  $M$  over  $Z_2$  [another nice basis is  $nb = \{(f^k)(\alpha^{(-1)})\}, k = 0 \dots 5\} = \{\alpha^{(-1)}, \alpha^{(-2)}, \alpha^{(-4)}, \alpha^{(-8)}, \alpha^{(-16)}, \alpha^{(-32)}\}$ , which is normal, that is, which is as a whole invariant under  $Gal$ , the Galois group generated by  $f$ ]. Now addition is easy (just add binary vectors, of length 6, modulo 2) and so is multiplication, for  $M^*$  is cyclic. Let us create a log-table to relate the two operations. This can be done recursively by hand. If  $[\alpha^i]_s = [x_1, x_2, x_3, x_4, x_5, x_6]$  ( $x_i \in Z_2$ ), then  $[\alpha^{(i+1)}]_s = [x_6, x_1 + x_6, x_2, x_3, x_4, x_5]$ . We give an example first, involving the two elements  $\beta$  and  $\delta$  (of multiplicative order 3 and 7), which generate the subfields  $K$  (of order 4) and  $L$  (of order 8), respectively.

```
> print('beta'=beta, 'beta'=Normal(beta) mod 2, 'delta'=delta, 'delta'=Normal(delta) mod 2);
```

$$\beta = \alpha^{21}, \beta = \alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1, \delta = \alpha^9, \delta = \alpha^4 + \alpha^3$$

We use an 8 x 8 matrix  $Lg$  to store the data compactly. Please ensure that your window is large enough for a proper display.

```
> with(linalg):Lg:=matrix(16,4,[ ]):
co:=p->[seq(coeff(p,alpha,k),k=0..5)]:srep:=x->co(Normal(x) mod 2):
print(['beta'] [s]=srep(beta), ['delta'] [s]=srep(delta));
```

Warning, the protected names norm and trace have been redefined and unprotected

$$[\beta]_s = [1, 1, 0, 1, 1, 1], [\delta]_s = [0, 0, 0, 1, 1, 0]$$

```
> A:=matrix(6,6,
[srep(alpha^(-1)),srep(alpha^(-2)),srep(alpha^(-4)),
srep(alpha^(-8)),srep(alpha^(-16)),srep(alpha^(-32))]):
det(A)mod 2;
```

1

We verified that  $nb$  is a basis indeed. Note that  $\alpha$  is *not* contained in a normal basis. The trace of  $\alpha$  is equal to zero, since the coefficient of  $X^5$  in  $p(X) = X^6 + X + 1$  is zero. The minimal polynomial of  $\alpha^{(-1)}$  is  $X^6 + X^5 + 1$ , the reciprocal of  $p(X)$ .

The trace is a linear mapping from  $M$  onto  $Z_2$  (with matrix, with respect to  $s$ , given by  $[1 \ 1 \ 1 \ 1 \ 1 \ 0]$ ) and can be defined by  $\text{trace}(t) = t + f(t) + (f^2)(t) + (f^3)(t) + (f^4)(t) + (f^5)(t)$ . Half of the elements of  $M$  have trace 0, the others trace 1.

All elements with trace zero are of the form  $x - f(x)$  so a telescoping argument might also have been applied.

```
> for j from 1 to 4 do for i from 1 to 16 do
Lg[i,j]:= [alpha^(i-1+16*(j-1))] [s] =
srep(alpha^(i-1+16*(j-1))) od od: Lg[16,4]:=[0] [s]=[0,0,0,0,0,0];
> evalm(Lg);
```

$[\alpha^1]_s = [1, 0, 0, 0, 0, 0]$	$[\alpha^{16}]_s = [1, 1, 0, 0, 1, 0]$	$[\alpha^{32}]_s = [1, 0, 0, 1, 0, 0]$	$[\alpha^{48}]_s = [1, 0, 1, 1, 0, 0]$
$[\alpha^2]_s = [0, 1, 0, 0, 0, 0]$	$[\alpha^{17}]_s = [0, 1, 1, 0, 0, 1]$	$[\alpha^{33}]_s = [0, 1, 0, 0, 1, 0]$	$[\alpha^{49}]_s = [0, 1, 0, 1, 1, 0]$
$[\alpha^3]_s = [0, 0, 1, 0, 0, 0]$	$[\alpha^{18}]_s = [1, 1, 1, 1, 0, 0]$	$[\alpha^{34}]_s = [0, 0, 1, 0, 0, 1]$	$[\alpha^{50}]_s = [0, 0, 1, 0, 1, 1]$
$[\alpha^4]_s = [0, 0, 0, 1, 0, 0]$	$[\alpha^{19}]_s = [0, 1, 1, 1, 1, 0]$	$[\alpha^{35}]_s = [1, 1, 0, 1, 0, 0]$	$[\alpha^{51}]_s = [1, 1, 0, 1, 0, 1]$
$[\alpha^5]_s = [0, 0, 0, 0, 1, 0]$	$[\alpha^{20}]_s = [0, 0, 1, 1, 1, 1]$	$[\alpha^{36}]_s = [0, 1, 1, 0, 1, 0]$	$[\alpha^{52}]_s = [1, 0, 1, 0, 1, 0]$
$[\alpha^6]_s = [0, 0, 0, 0, 0, 1]$	$[\alpha^{21}]_s = [1, 1, 0, 1, 1, 1]$	$[\alpha^{37}]_s = [0, 0, 1, 1, 0, 1]$	$[\alpha^{53}]_s = [0, 1, 0, 1, 0, 1]$
$[\alpha^7]_s = [1, 1, 0, 0, 0, 0]$	$[\alpha^{22}]_s = [1, 0, 1, 0, 1, 1]$	$[\alpha^{38}]_s = [1, 1, 0, 1, 1, 0]$	$[\alpha^{54}]_s = [1, 1, 1, 0, 1, 0]$
$[\alpha^8]_s = [0, 1, 1, 0, 0, 0]$	$[\alpha^{23}]_s = [1, 0, 0, 1, 0, 1]$	$[\alpha^{39}]_s = [0, 1, 1, 0, 1, 1]$	$[\alpha^{55}]_s = [0, 1, 1, 1, 0, 1]$
$[\alpha^9]_s = [0, 0, 1, 1, 0, 0]$	$[\alpha^{24}]_s = [1, 0, 0, 0, 1, 0]$	$[\alpha^{40}]_s = [1, 1, 1, 1, 0, 1]$	$[\alpha^{56}]_s = [1, 1, 1, 1, 1, 0]$
$[\alpha^{10}]_s = [0, 0, 0, 1, 1, 0]$	$[\alpha^{25}]_s = [0, 1, 0, 0, 0, 1]$	$[\alpha^{41}]_s = [1, 0, 1, 1, 1, 0]$	$[\alpha^{57}]_s = [0, 1, 1, 1, 1, 1]$
$[\alpha^{11}]_s = [0, 0, 0, 0, 1, 1]$	$[\alpha^{26}]_s = [1, 1, 1, 0, 0, 0]$	$[\alpha^{42}]_s = [0, 1, 0, 1, 1, 1]$	$[\alpha^{58}]_s = [1, 1, 1, 1, 1, 1]$
$[\alpha^{12}]_s = [1, 1, 0, 0, 0, 1]$	$[\alpha^{27}]_s = [0, 1, 1, 1, 0, 0]$	$[\alpha^{43}]_s = [1, 1, 1, 0, 1, 1]$	$[\alpha^{59}]_s = [1, 0, 1, 1, 1, 1]$
$[\alpha^{13}]_s = [1, 0, 1, 0, 0, 0]$	$[\alpha^{28}]_s = [0, 0, 1, 1, 1, 0]$	$[\alpha^{44}]_s = [1, 0, 1, 1, 0, 1]$	$[\alpha^{60}]_s = [1, 0, 0, 1, 1, 1]$
$[\alpha^{14}]_s = [0, 1, 0, 1, 0, 0]$	$[\alpha^{29}]_s = [0, 0, 0, 1, 1, 1]$	$[\alpha^{45}]_s = [1, 0, 0, 1, 1, 0]$	$[\alpha^{61}]_s = [1, 0, 0, 0, 1, 1]$
$[\alpha^{15}]_s = [0, 0, 1, 0, 1, 0]$	$[\alpha^{30}]_s = [1, 1, 0, 0, 1, 1]$	$[\alpha^{46}]_s = [0, 1, 0, 0, 1, 1]$	$[\alpha^{62}]_s = [1, 0, 0, 0, 0, 1]$
$[\alpha^{16}]_s = [0, 0, 0, 1, 0, 1]$	$[\alpha^{31}]_s = [1, 0, 1, 0, 0, 1]$	$[\alpha^{47}]_s = [1, 1, 1, 0, 0, 1]$	$[0]_s = [0, 0, 0, 0, 0, 0]$

For some practical purposes this is still not good enough. Another way to perform the calculations is by using a list of  $(64-2)/2=31$  unordered pairs  $\{i, j\}$  with the property that  $\alpha^i + \alpha^j = 1$ . Such a list can be easily calculated by hand with the help of the Frobenius morphism  $f$ . We get the following orbits of pairs (with lengths dividing 6, the order of  $f$ ) by starting with the pair  $(1,6)$  that defines  $M$  and the one that defines  $K$ . The last orbits are related to  $L$  and the multiplicative subgroup of order 9.

```
> pairs:=proc(a::integer,b::integer)
  local x, S::set;
  x:={a mod 63,b mod 63}: S:={}:
  while not member(x,S) do S:=S union {x}: x:=map(F,x) od:S;
end:
> pairs(1,6);pairs(-1,5);pairs(-5,-6);pairs(21,42);
      {{1, 6}, {2, 12}, {4, 24}, {8, 48}, {16, 33}, {3, 32}}
      {{5, 62}, {10, 61}, {20, 59}, {31, 34}, {40, 55}, {17, 47}}
      {{29, 60}, {39, 43}, {51, 53}, {57, 58}, {30, 46}, {15, 23}}
      {{21, 42}}
> pairs(9,45);pairs(7,26);pairs(-19,-26);
      {{9, 45}, {18, 27}, {36, 54}}
      {{7, 26}, {14, 52}, {28, 41}, {19, 56}, {38, 49}, {13, 35}}
      {{22, 50}, {37, 44}, {11, 25}}
```

An example should demonstrate the method in which addition is reduced to multiplication.

$$\alpha^7 + \alpha^{17} + \alpha^{29} = \alpha^7(1 + \alpha^{10} + \alpha^{22}) \stackrel{\{22,50\}}{=} \alpha^7(\alpha^{10} + \alpha^{50}) = \alpha^{17}(1 + \alpha^{40}) \stackrel{\{40,55\}}{=} \alpha^{72} = \alpha^9$$

From the last orbit of pairs (of length 3) we can conclude that the roots of the minimal polynomial  $X^6 + X^5 + X^3 + X^2 + 1$  of  $\alpha^{11}$  over  $Z_2$  satisfy three linear dependence relations of weight 4, for instance  $\alpha^{11} + \alpha^{22} + \alpha^{25} + \alpha^{50} = 0$ , so  $\alpha^{11}$  does not belong to a normal basis over  $Z_2$ . [the root sets of the remaining four over  $Z_2$  irreducible polynomials of degree 6 containing  $X^5$  each do constitute a normal basis, as a Maple calculation might show]

```
> Expand((X+alpha^11)*(X+alpha^22)*(X+alpha^44)*(X+alpha^25)*(X+alpha^50)*(X+alpha^37)
)mod 2;
      X^5 + X^2 + X^3 + X^6 + 1
```

Minimal polynomials of elements of  $M$  can be determined by standard linear algebra methods: "Find the first linear dependence that occurs between the sequence of its successive powers". For instance for  $\delta$  we get:

```
> D1:=transpose(matrix(4,6,[srep(1),srep(delta),srep(delta^2),srep(delta^3)])):
kernel(D1);
```

{[1, 0, -1, 1]}

The minimal polynomial of  $\delta$  is  $1 - X + X^3 = 1 + X + X^3$  with degree 3, indeed. In general:

```
> lin:=proc(x)
  local i,A::matrix,B,K: A:=matrix(0,6,[]):
  for i from 0 to 6 do A:=stackmatrix(A,srep(x^i)) od:
  B:=transpose(A):K:=kernel(B):
  map(fmap,K) end:
> epsilon:=alpha^7: lin(epsilon);
```

{[1, 0, 0, 1, 0, 0, 1]}

Hence the minimal polynomial of  $\epsilon = \alpha^7$  is  $1 + X^3 + X^6$ , which comes not unexpected. For  $\epsilon$  is a third root of  $\beta$ , or since  $\epsilon$  has order 9, it is a root of  $X^9 - 1 = (X^3 - 1)(X^6 + X^3 + 1)$ . Let us now factorize this polynomial over  $M$ , as well as over its proper subfields  $K$  and  $L$ . As Galois theory predicts the linear factors over  $M$  can be grouped together according to the orbits of the two cyclic subgroups of  $Gal$  generated by  $f^3$  and  $f^2$ , respectively. We have to introduce two dummies, one for beta and one for delta.

```
> alias(_beta=RootOf(X^2+X+1)):alias(_delta=RootOf(X^3+X^2+1)):
```

```
> orb:=proc(k)
  local N::list,j,i::posint:
  i:=1: j:=k: N:=[:
  while i<7 do N:=[op(N),alpha^j=Normal(alpha^j) mod 2]:
  j:=F(j):i:=i+1:
od: N:
end:
orb(7);
```

$[\alpha^7 = \alpha^2 + \alpha, \alpha^{14} = \alpha^4 + \alpha^2, \alpha^{28} = \alpha^4 + \alpha^3 + \alpha^2, \alpha^{56} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1, \alpha^{49} = \alpha^4 + \alpha^3 + \alpha, \alpha^{35} = \alpha^3 + \alpha + 1]$

```
> Factor(X^6+X^3+1,alpha) mod 2;
```

$(X + \alpha^3 + \alpha + 1)(X + \alpha^2 + \alpha)(X + \alpha^4 + \alpha^3 + \alpha)(X + \alpha^4 + \alpha^3 + \alpha^2)(X + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1)(X + \alpha^4 + \alpha^2)$

```
> Factor(X^6+X^3+1,_beta)mod 2;
```

```
'X^3+beta+1'=Factor(X^3+beta+1,alpha)mod 2;
```

```
'X^3+beta'=Factor(X^3+beta,alpha)mod 2;
```

$(X^3 + \beta + 1)(X^3 + \beta)$

$X^3 + \beta + 1 = (X + \alpha^3 + \alpha + 1)(X + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1)(X + \alpha^4 + \alpha^2)$

$X^3 + \beta = (X + \alpha^2 + \alpha)(X + \alpha^4 + \alpha^3 + \alpha)(X + \alpha^4 + \alpha^3 + \alpha^2)$

```
> Factor(X^6+X^3+1,_delta)mod 2;
```

```
'X^2+(delta+1)*X+1'=Factor(X^2+(delta+1)*X+1)mod 2;
```

```
'X^2+(delta^2+delta)*X+1'=Factor(X^2+(delta^2+delta)*X+1)mod 2;
```

```
'X^2+(delta^2+1)*X+1'=Factor(X^2+(delta^2+1)*X+1)mod 2;
```

$(X^2 + (\delta^2 + 1)X + 1)(X^2 + (\delta + 1)X + 1)(X^2 + (\delta^2 + \delta)X + 1)$

$X^2 + (\delta + 1)X + 1 = (X + \alpha^2 + \alpha)(X + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1)$

$X^2 + (\delta^2 + \delta)X + 1 = (X + \alpha^3 + \alpha + 1)(X + \alpha^4 + \alpha^3 + \alpha^2)$

$X^2 + (\delta^2 + 1)X + 1 = (X + \alpha^4 + \alpha^2)(X + \alpha^4 + \alpha^3 + \alpha)$

Finally, all irreducible polynomials over  $Z_2$  of degree 1, 2, 3, or 6 are contained (exactly once) in  $g_{64}(X)$ :

```
> Factor(X^64-X)mod 2;
```

$(1 + X^3 + X^2)(X^6 + X^3 + 1)(X^3 + X + 1)(X^6 + X^5 + 1)(X^6 + X^5 + X^3 + X^2 + 1)(X^6 + X + 1)(X^6 + X^4 + X^2 + X + 1)$

$(X + 1 + X^2)(X^6 + X^5 + X^4 + X + 1)(X + 1)(X^6 + X^4 + X^3 + X + 1)(X^6 + X^5 + X^2 + X + 1)X(X^6 + X^5 + X^4 + X^2 + 1)$

```
> Factor(X^8-X)mod 2;Factor(X^4-X)mod 2;
```

$(1 + X^3 + X^2)(X^3 + X + 1)(X + 1)X$

$(X + 1 + X^2)(X + 1)X$

The norm of all nonzero elements is equal to 1, the only nonzero element in  $Z_2$ . If we define the norm  $n(t)$  of  $t$ , by

$n(t) = t f(t) (f^2)(t) (f^3)(t) (f^4)(t) (f^5)(t) \dots = t^{(1+2+4+8+16+32)+\dots} = t^{63} = 1$ , the constant coefficient (or a

power of it) of the minimal polynomial of  $t$  (not equal to 0). We might also use a telescoping argument again:  $t = u/f(u)$  for  $u = 1/t$ .