

## 5. FINITE FIELDS

On the last day I asked several questions about  $\mathbb{F}_{2^8}$  and we tried to answer them.

**5.1. Galois group.** The first question was: What is the Galois group of  $\mathbb{F}_{2^8}/\mathbb{F}_2$ ? Since  $\mathbb{F}_{2^8}$  is a vector space of dimension 8 over  $\mathbb{F}_2$ , its degree is 8. So,  $Gal(\mathbb{F}_{2^8}/\mathbb{F}_2)$  has 8 elements. Which group is it?

To answer this we looked for intermediate fields. If  $\mathbb{F}_q$  is contained in  $\mathbb{F}_{2^8}$  then  $2^8 = q^n$  for some  $n \geq 1$ . So,  $q = 1, 2, 2^2, 2^4, 2^8$ . So, there are only two intermediate fields:  $\mathbb{F}_4, \mathbb{F}_{16}$ . This means the Galois group has exactly 2 nontrivial proper subgroups. So, it must be cyclic.

$$Gal(\mathbb{F}_{2^8}/\mathbb{F}_2) \cong \mathbb{Z}/8.$$

In fact the Galois group of any finite field is cyclic.

**Theorem 5.1.** *The Galois group of  $\mathbb{F}_{p^n}/\mathbb{F}_p$  is a cyclic group of order  $n$  generated by the Frobenius*

$$\phi(x) = x^p.$$

*Proof.* The Frobenius is a homomorphism  $\phi : K \rightarrow K$  for any field  $K$  of characteristic  $p$ . Its kernel is trivial since  $x^p = 0$  implies  $x = 0$ . Therefore,  $\phi$  is an automorphism for any finite field. So, it is an element of the Galois group. The fixed field of this element is the set of all roots of

$$X^p - X$$

But the  $p$  elements of the prime field  $\mathbb{F}_p$  are roots of this polynomial. So

$$\mathbb{F}_p = \mathbb{F}_p^{\langle \phi \rangle}.$$

By the Galois correspondence, this implies that  $\langle \phi \rangle = Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$ .  $\square$

**Corollary 5.2.**  *$Gal(\mathbb{F}_{p^{nm}}/\mathbb{F}_{p^n})$  is the cyclic group generated by  $\phi^n$ .*

**5.2. the field  $\mathbb{F}_4$ .** has only 4 elements:  $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$ .

**Proposition 5.3.** *The irreducible polynomial of  $\alpha$  is*

$$X^2 + X + 1.$$

*Proof.* 0, 1 are not roots of this polynomial. So, the polynomial is irreducible and defines a degree 2 extension of  $\mathbb{F}_2$ .

In class I gave another proof. There are only 4 polynomials of degree 2: the one above and

$$X^2 + X, \quad X^2 + 1, \quad X^2.$$

But these polynomials are not irreducible:

$$X^2 + X = X(X + 1), \quad X^2 + 1 = (X + 1)^2$$

So,  $X^2 + X + 1$  is the unique degree 2 irreducible polynomial over  $\mathbb{F}_2$ . So, it must be the irreducible polynomial of  $\alpha$ .  $\square$

If we were to represent elements of  $\mathbb{F}_4$  in binary notation we would write the elements as: (0, 0), (0, 1), (1, 0), (1, 1) where

$$(0, 0) = 0, \quad (0, 1) = 1, \quad (1, 0) = \alpha, \quad (1, 1) = \alpha + 1.$$

Addition is coordinate-wise and multiplication is given by the irreducible polynomial.

**5.3. the field  $\mathbb{F}_{16}$ .** We know that  $\mathbb{F}_{16} = \mathbb{F}_4(\beta)$  for any element  $\beta$  of  $\mathbb{F}_{16}$  which is not in  $\mathbb{F}_4$ . We want the irreducible polynomial of  $\beta$  over  $\mathbb{F}_2$  since this will let us write elements of  $\mathbb{F}_{16}$  as strings of four 0's and 1's and tell us how to multiply them.

The irreducible polynomial of  $\beta$  over  $\mathbb{F}_4$  is quadratic. One possibility is

$$f(X) = X^2 + X + \alpha.$$

The four elements of  $\mathbb{F}_4$  are not roots of this polynomial. So, it is irreducible. If  $\beta$  is a root then the irreducible polynomial of  $\beta$  over  $\mathbb{F}_2$  is

$$f\bar{f} = (X^2 + X + \alpha)(X^2 + X + \bar{\alpha})$$

where conjugation  $\bar{\alpha}$  is given by the element of the Galois group,  $\phi$ . So,  $\bar{\alpha} = \phi(\alpha) = \alpha^2 = \alpha + 1$  and

$$\begin{aligned} \text{irr}(\beta, \mathbb{F}_2) &= (X^2 + X + \alpha)(X^2 + X + \alpha + 1) = (X^2 + X + \alpha)^2 + (X^2 + X + \alpha) \\ &= X^4 + X^2 + \alpha + 1 + X^2 + X + \alpha = X^4 + X + 1. \end{aligned}$$

This polynomial has 4 roots. Since  $\mathbb{F}_{16}$  has  $16 - 4 = 12$  generators and each degree 4 irreducible polynomial has 4 roots, there must be two more irreducible polynomials.

**Theorem 5.4.** *There are exactly three irreducible degree 4 polynomials over  $\mathbb{F}_2$ :*

- (1)  $f_1(X) = X^4 + X + 1$
- (2)  $f_2(X) = X^4 + X^3 + 1$
- (3)  $f_3(X) = X^4 + X^3 + X^2 + X + 1$ .

*Proof.* There are only 8 polynomial of degree 4 with nonzero constant term. The other 5 are reducible since:

$$X^4 + 1, X^4 + X^2 + X + 1, X^4 + X^3 + X + 1, X^4 + X^3 + X^2 + 1$$

have an even number of terms and thus have  $X = 1$  as a root and

$$X^4 + X^2 + 1 = (X^2 + X + 1)^2.$$

I also pointed out that  $f_2$  is the reverse of  $f_1$  and is thus irreducible (the roots of  $f_2$  are the inverses of the roots of  $f_1$ ). The roots of  $f_3$  are 5th roots of unity, so they are not elements of  $\mathbb{F}_4$ .  $\square$

Here is an example of how multiplication is done in  $\mathbb{F}_{16}$  using the irreducible polynomial  $X^4 + X + 1$ .

$$(1101)(0101) = 1101 + 11, 0100 = 11, 1001 = 1, 1111 = 1100$$

where the last two reductions use the irreducible polynomial which is 1,0011:

$$11, 1001 = 11, 1001 + 10, 0110 = 1, 1111 = 1, 1111 + 1, 0011 = 1100.$$

The commas are just to make it easier to read the numbers.

5.4. **the field  $\mathbb{F}_{256}$ .** We didn't get very far with this. The usual irreducible polynomial is

$$g(X) = X^8 + X^7 + X^2 + X + 1 = 1, 1000, 0111$$

5.4.1. *number of irreducible polynomials.* The number of irreducible polynomials of degree 8 is

$$\frac{256 - 16}{8} = \frac{240}{8} = 30.$$

The number of polynomials of degree 8 with nonzero constant term is  $2^7 = 128$ . Half of these have an even number of terms making  $X = 1$  a root. This leaves 64. There are  $2^5 = 32$  polynomials which have  $\alpha$  as a root and half of them have an odd number of terms. This leaves  $64 - 16 = 48$ . We can multiply any two of the three irreducible degree 4 polynomials. There are 6 ways to do that. This leaves 42 left. There are two irreducible polynomials of degree 3, namely,

$$X^3 + X + 1, \quad X^3 + X^2 + 1.$$

And there are 6 irreducible polynomials of degree 5. (Three are 8 polynomials of degree 5 with nonzero constant term and an odd number of terms. Two of them factor as  $X^2 + X + 1$  times one of the two degree 3 irreducibles.) This makes  $2 \cdot 6 = 12$  products leaving  $42 - 12 = 30$  irreducible polynomials of degree 8.

5.4.2. *irreducible polynomial over intermediate fields.* Let  $\gamma$  be a root of the polynomial  $g(X)$ . Then what is the irreducible polynomial of  $\gamma$  over  $\mathbb{F}_4$ ? over  $\mathbb{F}_{16}$ ?

Since  $\phi^4$  generates the Galois group of  $\mathbb{F}_{2^8}/\mathbb{F}_{16}$ , the polynomial of  $\gamma$  over  $\mathbb{F}_{16}$  is

$$(X - \gamma)(X - \phi^4(\gamma)) = (X - \gamma)(X - \gamma^{16}) = X^2 + (\gamma + \gamma^{16})X + \gamma^{17}.$$

Using a computer, I calculated this in binary notation:

$$\gamma^{17} = 1101, 1110, \quad \gamma^{16} = 0110, 1111.$$

So,

$$\text{irr}(\gamma, \mathbb{F}_{16}) = X^2 + 0110, 1101X + 1101, 1110.$$

Some further computer calculations show that

$$\alpha = 1010, 1010, \quad \beta = 1101, 1110$$

satisfy the equations:

$$\alpha^2 + \alpha = 1, \quad \beta^2 + \beta = \alpha, \quad \beta^4 + \beta = 1.$$

So, we can identify them with the generators of  $\mathbb{F}_4$  and  $\mathbb{F}_{16}$  that we chose earlier. In this notation we have:

$$\text{irr}(\gamma, \mathbb{F}_{16}) = X^2 + (\alpha + 1)(\beta + 1)X + \beta.$$

Applying the generator  $\phi^2$  of  $\text{Gal}(\mathbb{F}_{16}/\mathbb{F}_4)$  we get

$$\text{irr}(\gamma^4, \mathbb{F}_{16}) = X^2 + (\alpha + 1)\beta X + \beta + 1$$

The product of these is

$$\text{irr}(\gamma, \mathbb{F}_4) = X^4 + \bar{\alpha}X^3 + \alpha X^2 + \bar{\alpha}X + \alpha.$$

If we multiply this with the conjugate:

$$\text{irr}(\gamma^2, \mathbb{F}_4) = X^4 + \alpha X^3 + \bar{\alpha}X^2 + \alpha X + \bar{\alpha}$$

we get back the original irreducible polynomial

$$\text{irr}(\gamma, \mathbb{F}_2) = X^8 + X^7 + X^2 + X + 1.$$

5.4.3. *the order of  $\gamma$ .* One last point: The calculation

$$\gamma^{17} = \beta$$

implies that  $\gamma$  is a generator of the cyclic group

$$\mathbb{F}_{256}^\times \cong \mathbb{Z}/255 \cong \mathbb{Z}/17 \oplus \mathbb{Z}/5 \oplus \mathbb{Z}/3$$

since  $\beta$  has order 15. (The elements of order 3 lie in  $\mathbb{F}_4$  and the elements of order 5 are roots of the irreducible polynomial  $f_3(X)$ .  $\beta$  is a root of  $f_1(X)$ .)