

**33.3. units and polynomials.** In both theory and practice it is important to use polynomials to work with finite fields. In the example of  $GF(16)$  each element is written as a sequence of 4 binary digits:

$$c_3c_2c_1c_0$$

where  $c_0, c_1, c_2, c_3$  are elements of  $GF(2) = \mathbb{Z}_2 = \{0, 1\}$ . But this notation represents the polynomial:

$$p(\alpha) = c_3\alpha^3 + c_2\alpha^2 + c_1\alpha + c_0$$

I will explain the bare minimum of the theory of polynomials with coefficients in an arbitrary field so that we can use this idea to handle arbitrary finite fields.

**Definition 33.5.** *Suppose that  $F$  is any field. Then a polynomial with coefficients in  $F$  is a formal expression:*

$$f(X) = c_nX^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0$$

where each  $c_i$  is an element of  $F$  and  $c_n \neq 0$  ( $c_n$  is called the **leading coefficient** of  $f(X)$  and  $n$  is called the **degree** of the polynomial  $f(X)$ ). Addition and multiplication of polynomials is given in the usual way keeping in mind that the coefficients are elements of  $F$ . The set of all such polynomials is denoted  $F[X]$  and is called the **polynomial ring** in the variable  $X$  with coefficients in  $F$ .

It is very important that square brackets are used in the notation because  $F(X)$  means something else.

Here is an example to remind you how polynomials are added and multiplied. Take  $F = \mathbb{Z}_3$

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

$$(X - 1)^3 = (X + 2)^3 = X^3 + 6X^2 + 12X + 8 = X^3 + 2$$

Note that we can eliminate any minus signs since, e.g.,  $-1 = 2$  in  $\mathbb{Z}_3$ .

Problem: Show that  $F[X]$  is an integral domain (commutative with unity and no zero divisors). Hint: The leading coefficient of  $f(X)g(X)$  is the product of the leading coefficients of  $f(X)$  and of  $g(X)$ .

Problem: Show that  $F[X]$  has the same characteristic as  $F$ .

**Definition 33.6.** *A polynomial  $f(X)$  is called **monic** if its leading coefficient is 1.*

The reason that monic polynomials are important is because we can divide by them. Here is an example and a theorem which I feel is so obvious that it hardly requires proof.



If we insert any  $\beta_i$  for  $X$  we get:

$$f(\beta_i) = 0 = (\beta_i - \alpha)q(\beta_i)$$

Since  $\beta_i \neq \alpha$  we must have

$$q(\beta_i) = 0$$

But this makes  $q(X)$  into a polynomial of degree  $n - 1$  with  $n$  different roots which is not possible by the induction hypothesis. This proves the corollary.  $\square$

**Theorem 33.10.** *If  $F$  is a finite field of order  $q$  then  $F^\times$  is a cyclic group of order  $q - 1$ .*

In lieu of a proof, I will explain why this is true using two examples. Take  $q = 9$ . Then  $F^\times$  has 8 elements. So, every element has order a power of 2 (since  $o(g)$  divides  $|G|$  for any  $g \in G$ ). If  $F^\times$  is not cyclic then its elements all have order 2 or 4. This means that the polynomial

$$X^4 - 1$$

has 8 different roots which is impossible by the corollary we just proved.

Next, take  $q = 25$ . Then  $F^\times$  has  $24 = 3 \cdot 8$  elements. If the orders of the elements divide 12 then the polynomial  $X^{12} - 1$  has 24 roots which is impossible. So,  $F^\times$  has an element  $x$  of order 24 or an element  $\alpha$  of order 8 (these are the only two divisors of 24 which do not divide 12). But then  $\alpha = x^3$  has order 8. So, in both cases we get an element  $\alpha$  of order 8. Similarly,  $F^\times$  has an element  $\beta$  of order 3.

Claim: The product  $\alpha\beta$  has order 24 and therefore  $F^\times$  is cyclic.

To prove this suppose that  $o(\alpha\beta) = n$ . Then

$$(\alpha\beta)^n = \alpha^n\beta^n = 1$$

which implies that  $\beta^n = \alpha^{-n}$ . Cubing both gives  $\beta^{3n} = \alpha^{-3n} = 1$  which implies the order of  $\beta$  divides  $3n$ . So:

$$8|3n \Rightarrow 8|n$$

Also  $\alpha^{-8n} = \beta^{8n} = 1$  which implies the order of  $\alpha$  divides  $8n$ . So

$$3|8n \Rightarrow 3|n \Rightarrow 24|n$$

So,  $\alpha\beta$  has order 24.

Other cases are similar. But I won't go through the proof. It uses the following lemma which was illustrated in the second example we just did.

**Lemma 33.11.** *If  $G$  is an abelian group and  $\alpha, \beta \in G$  have order  $n, m$  which are relatively prime then  $\alpha\beta$  has order  $nm$ .*