# Basics on Finite Fields

Recall that $\mathcal{F}$ is a field if and only if

(i) $\mathcal{F}$ it has two operations "+" and "×" and two elements "0" and "1" such that both $(\mathcal{F},\text{"+ "})$ and $(\mathcal{F}-\{0\},\text{"×"})$ are abelian groups

(ii) For all $x,y,z\in\mathcal{F}$ we have

$$x(y+z) \;=\; (y+z)x \;=\; xy+xz \;=\; yx+zx\,.$$

Note that the finiteness of $\mathcal{F}$ implies that the infinite sequence

$$1\,,\quad 1+1\,,\quad 1+1+1\,,\quad 1+1+1+1\,,\quad \ldots$$

must contains only a finite number of distinct elements. Denoting by "$k$" the $k^{th}$ element of this sequence, then for some $h<k$ we must have $h=k$. This forces $k-h=0$ in $\mathcal{F}$. Recall that the integer

$$p \;=\; \min\{k\,:\,k=0 \text{ in } \mathcal{F}\}$$

is called the " *characteristic of* $\mathcal{F}$ ". It is easily seen that

(iii) $k=0$ in $\mathcal{F}$ if and only if $p$ divides $k$

(iv) $p$ is a prime number.

In fact, note that if $k=0$ in $\mathcal{F}$ then the definition of $p$ forces $k\geq p$ and if $k>p$ then we can find two integers $Q$ and $R$ such that $k=Qp+R$ with $R<p$ yielding that $R=0$ in $\mathcal{F}$. But then $R>0$ would contradict the definition of $p$, proving (iii). Likewise if $p=ab$ with $a,b>1$ then $a\neq 0$ in $\mathcal{F}$ and the fact that $(\mathcal{F}-\{0\},\text{"×"})$ is a group would give

$$a^{-1}p \;=\; b \qquad (\text{in } \mathcal{F})$$

forcing $b=0$ in $\mathcal{F}$, again contradicting the definition of $p$. Clearly we are led to the same conclusion if $b\neq 0$ in $\mathcal{F}$. This proves (iv).

Throughout the rest of this section $\mathcal{F}$ will denote a finite field and $q$ its cardinality.

Before we can proceed with deeper properties of finite fields we must acquire some basic tools for working with polynomials. These will be presented in separate subsections.

### 1.1 The Euclidean algorithm

The original Euclidean algorithm was a process which yielded the greatest common divisor $d$ of two given integers $A$ and $B$. We shall use it here for the the ring of integers as well as for the ring of polynomials in a single variable $x$ with coefficients in a field. We shall present here a modified version of the Euclidean algorithm due to Berlekamp [] which is extremely elegant and very suitable for explicit computations of greatest common divisors. For the rest of this section all the elements we deal with are supposed to belong to some fixed ring $\mathcal{R}$ with $\mathcal{R}=\mathbb{Z}$ or $\mathcal{R}=\mathcal{F}[x]$ for some field $\mathcal{F}$. In order to use the same terminology in any of these cases, we let $degree(a)=ln|a|$ for $a\in\mathbb{Z}$ and $degree(a)$ mean the ordinary degree of a polynomial when $a\in\mathcal{F}[x]$.

We recall, that the greatest common divisor of two elements $A,B\in\mathcal{R}$ is denoted $(A,B)$ and we say that $A$ and $B$ are "*relatively prime*" if and only if $(A,B)=1$,

This given, to compute the greatest common divisor $(A, B)$ by the Berlekamp algorithm we start by setting

$$r_{-2} = A \quad , \quad r_{-1} = B \quad , \quad p_{-2} = 0 \quad , \quad p_{-1} = 1 \quad , \quad q_{-2} = 1 \quad , \quad q_{-1} = 0 \tag{1.1}$$

then compute $a_k, r_k, p_k, q_k$ according to the recursions (**)

$$\begin{aligned} &(i) \quad r_{k-2} \;=\; a_k\, r_{k-1} \;+\; r_k \quad (\textit{by the division algorithm}) \\ &(ii) \quad p_k \;=\; a_k\, p_{k-1} \;+\; p_{k-2} \qquad . \qquad (\ k = 0, 1, 2, \dots\ ) \\ &(iii) \quad q_k \;=\; a_k\, q_{k-1} \;+\; q_{k-2} \end{aligned} \tag{1.2}$$

since the degree of $r_k$ decreases at least by one at each step after $n < B$ steps we shall have $r_n = 0$. we will show that these recursions force the following basic identities

$$\begin{aligned} &(a) \quad q_n\, p_{n-1} \,-\, p_n\, q_{n-1} \;=\; (-1)^n \\ &(b) \quad A \;=\; r_{n-1}\, p_n \\ &(c) \quad B \;=\; r_{n-1}\, q_n \\ &(d) \quad B\, p_{n-1} \,-\, A\, q_{n-1} \;=\; (-1)^n r_{n-1} \end{aligned} \qquad . \tag{1.3}$$

Clearly we need only establish (a), (b) and (c) since (d) is obtained by multiplying the first of these equations by $r_{n-1}$ and using 1.3 (b) and 1.3 (c).

Now note that (b) and (c) show that $r_{n-1}$ is a common divisor of $A$ and $B$, while (d) shows that any common divisor of $A$ and $B$ must divide $r_{n-1}$. Thus

$$(A, B) \;=\; r_{n-1}$$

and we may rewrite 1.3 (d) in the form

$$(A, B) \;=\; H\, A \,-\, K\, B \qquad \text{with} \quad \begin{cases} H = (-1)^{n-1} q_{n-1} \\ K = (-1)^{n-1} p_{n-1} \end{cases} \tag{1.4}$$

We should note that the advantage of this process over the one that is usually described in most textbooks is that it yields, not only the greatest common divisor of $A$ and $B$ but at the same time it constructs a pair of elements $p_{n-1}, q_{n-1}$ yielding the expansion in 1.4 expressing $(A, B)$ as a linear combination of $A$ and $B$. Moreover it does all this without the neeed of excessive storage of partial results. In fact, only 6 results need to be stored at any particular time, a number that is independent of the choice of $A$ and $B$.

We should also mention that we can use the Euclidean Algorithm to construct the continued fraction expansion of any rational number. The basic identity here may be written as

$$\frac{A}{B} \;=\; a_0 \;+\; \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{\cdots}{\cdots \cfrac{\cdots}{a_{n-1} + \cfrac{1}{a_n}}}}}$$

(**) Given two elements $a, b \in \mathcal{R}$, the "division" of $a$ by $b$ consists in the construction of two elements $q, r \in \mathcal{R}$, yielding $a = bq + r$ (usually referred to as the "quotient" and the "remainder") and uniquely determined by the condition that $degree(r) < degree(b)$. .

To prove the validity of this algorithm we need only establish the relations in 1.3. To this end it is convenient to rewrite the recursions in 1.2 in matrix form. For instance we may write 1.2 (i) as

$$\begin{bmatrix} a_k & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} r_{k-1} \\ r_k \end{bmatrix} = \begin{bmatrix} r_{k-2} \\ r_{k-1} \end{bmatrix} . \tag{1.5}$$

Likewise 1.2 (ii) and (iii) can be simultaneously obtained from the single equation

$$\begin{bmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{bmatrix} = \begin{bmatrix} p_{k-1} & p_{k-2} \\ q_{k-1} & q_{k-2} \end{bmatrix} \times \begin{bmatrix} a_k & 1 \\ 1 & 0 \end{bmatrix} . \tag{1.6}$$

Setting $k = 0$ in 1.5 and using the initial conditions in 1.1 gives

$$\begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} B \\ r_0 \end{bmatrix} = \begin{bmatrix} A \\ B \end{bmatrix} . \tag{1.7}$$

Similarly, setting $k = 1$ in 1.5 we get

$$\begin{bmatrix} a_1 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} r_0 \\ r_1 \end{bmatrix} = \begin{bmatrix} B \\ r_0 \end{bmatrix} .$$

Now this may be used in 1.7 to give

$$\begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} a_1 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} r_0 \\ r_1 \end{bmatrix} = \begin{bmatrix} A \\ B \end{bmatrix} . \tag{1.8}$$

Next, setting $k = 2$ in 1.5 we get

$$\begin{bmatrix} a_2 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} r_1 \\ r_2 \end{bmatrix} = \begin{bmatrix} r_0 \\ r_1 \end{bmatrix} .$$

and using this in 1.8 gives

$$\begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} a_1 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} a_2 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} r_1 \\ r_2 \end{bmatrix} = \begin{bmatrix} A \\ B \end{bmatrix} .$$

This should make it clear that repeating this process $k$ times leads to the identity

$$\begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} a_1 & 1 \\ 1 & 0 \end{bmatrix} \times \cdots \times \begin{bmatrix} a_k & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} r_{k-1} \\ r_k \end{bmatrix} = \begin{bmatrix} A \\ B \end{bmatrix} . \tag{1.9}$$

Likewise, k repeated applications of the recurrence in 1.6 yields that

$$\begin{bmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{bmatrix} = \begin{bmatrix} p_{-1} & p_{-2} \\ q_{-1} & q_{-2} \end{bmatrix} \times \begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} a_1 & 1 \\ 1 & 0 \end{bmatrix} \times \cdots \times \begin{bmatrix} a_k & 1 \\ 1 & 0 \end{bmatrix} \tag{1.10}$$

Now the initial conditions in 1.1 give

$$\begin{bmatrix} p_{-1} & p_{-2} \\ q_{-1} & q_{-2} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

and 1.10 reduces to

$$\begin{bmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{bmatrix} \;=\; \begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} a_1 & 1 \\ 1 & 0 \end{bmatrix} \times \cdots \times \begin{bmatrix} a_k & 1 \\ 1 & 0 \end{bmatrix} \tag{1.11}$$

Using this in 1.9 we finally derive that

$$\begin{bmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{bmatrix} \times \begin{bmatrix} r_{k-1} \\ r_k \end{bmatrix} \;=\; \begin{bmatrix} A \\ B \end{bmatrix} . \tag{1.12}$$

Note that since the determinant of the product of any number of matrices is equal to the product of the determinants, from 1.11 we deduce that

$$p_k\, q_{k-1} - p_{k-1}\, q_k \;=\; (-1)^{k+1}$$

and this proves 1.3 (a). Now , if $r_n = 0$, then 1.12 for $k = n$ becomes

$$\begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix} \times \begin{bmatrix} r_{n-1} \\ 0 \end{bmatrix} \;=\; \begin{bmatrix} A \\ B \end{bmatrix}$$

which simultaneously gives 1.3 (b) and (c) and our argument is complete.

## Remark 1.1

Note that in the case that $A$ and $B$ are relatively prime the equation in 1.4 reduces to

$$1 \;=\; A\,(-1)^{n-1} q_{n-1} \;-\; B\,(-1)^n p_{n-1} \tag{$*$}$$

This crucial identity, which here and after will be referred to as the "*star identity*" , makes the Euclidean Algorithm a basic tool in the construction of inverses. To get accross what we have in mind here we shall go over standard example. It is easy to verify that for any integer $p$ the set of integers

$$\Omega_p \;=\; \{0\,,\; 1\,,\; 2\,,\; \ldots\,,\; p-1\}$$

form a ring when multiplication and addition are carried out "$mod\, p$". However, when $p$ is a prime then every element in $\Omega_p$, except 0, has an inverse. In fact, every one of these elements is prime with $p$, and the Euclidean Algorithm carried out with $A$ the given element and $B = p$ yields the identity

$$1 \;=\; A\,(-1)^{n-1} q_{n-1} \qquad (mod\;\; p)$$

and we may set

$$A^{-1} \;=\; (-1)^{n-1} q_{n-1}\,.$$

This given it is easy to verify that the set $\Omega_p$ together with this notion of inverse is actually a field. Here and after we shall denote this field "$\mathbb{F}_p$" and refer to it as a " *prime field* " . We should note that from the observations at the beginning of this section it follows that every field of characeristic $p$ contains $\mathbb{F}_p$ as a subfield.

### 1.2 Polynomial factorization.

It is good to begin with the following basic fact.

**Lemma 1.1**(Gauss)

*If a polynomial $P(x) = \sum_{m=0}^{n} p_m x^m$ with integer coefficients factors over the rationals then it factors over the integers*

**Proof**

Clearly there is no loss in assuming that the coefficients of $P(x)$ have no common factor. Now if $P(x)$ factors over the rationals, we shall have two polynomials $A(x) = \sum_{i=0}^{a} a_i\, x^i$ and $B(x) = \sum_{j=0}^{b} b_i\, x^i$ with rational coefficients yielding $P(x) = A(x)B(x)$. Now let $d_a$ be the least common multiple of the denominators of the $a_i$ and $d_b$ be the least common multiple of the denominators of the $b_j$. Let $R(x) = \sum_{i=0}^{a} r_i\, x^i = d_a A(x)$ and $S(x) = \sum_{j=0}^{b} s_i\, x^i = d_b B(x)$. Setting $M = d_a d_b$ we shall have the factorization

$$MP(x) \;=\; R(x)S(x)\,. \tag{1.13}$$

where $R(x)$ and $S(x)$ are polynomials with integer coefficients. Note further that if the coefficients of $R(x)$ have a common prime factor then this factor must divide $M$. Likewise $M$ must be divisible by any common prime factor of the coefficients of $S(x)$. This given, by successive divisions of both sides of 1.13 by all such prime factors we can reduce 1.13 to an equation where both $R(x)$ and $S(x)$ have coefficients that have no common factor.

This given, let $q$ be a prime factor of $M$. Equating constant terms in 1.13 gives

$$Mp_o \;=\; r_0 s_0$$

thus $q$ must divide $r_0$ or $s_0$ or both. Equating coefficients of $x$ in 1.13 gives

$$Mp_1 \;=\; r_0 s_1 + r_1 s_0$$

So if $q$ did divide $r_0$ then $q$ must divide $r_1 s_o$ and thus it must divide $r_1$, $s_0$ or both. From our assumptions $q$ cannot divide all of the $r_i's$ nor all of the $s_j's$. This given, let $i_o$ be the first $i$ such that $q$ does not divide $s_i$ and $j_o$ be the first $j$ such that $q$ does not divide $s_j$. But now let us equate coefficients of $x^{i_o+j_o}$ in 1.13. This gives

$$Mp_{i_o+j_o} \;=\; r_o\, s_{i_o+j_o} + r_1\, s_{i_0+j_o-1} + r_2\, s_{i_o+j_o-2} + \cdots + r_{i_o} s_{j_o} + \cdots + r_{i_o+j_o-2}\, s_2 + r_{i_o+j_o-1}\, s_1 + r_{i_o+j_o}\, s_o$$

But we immediately see a contradiction here since the left hand side is divisible by $q$, all terms preceding $r_{i_o} s_{j_o}$ and all terms following $r_{i_o} s_{j_o}$ are divisible by $q$ and by assumption $r_{i_o} s_{j_o}$ itself is not divisible by $q$. The contradiction arises from assuming that $M$ is other than $\pm 1$. This completes our proof.

**Lemma 1.2**

*In any field $\mathcal{F}$ a polynomial $P(x) \in \mathcal{F}[x]$ of degree $n$ cannot have more than $n$ roots.*

**Proof**

Let

$$P(x) \;=\; c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$$

then for any $\alpha \in \mathcal{F}$ we have

$$P(x) - P(\alpha) \;=\; \sum_{r=1}^{n} c_r \big(x^r - \alpha^r\big).$$

Since

$$x^r - \alpha^r \;=\; (x-\alpha)\sum_{s=0}^{r-1} x^s \alpha^{r-1-s}$$

it follows that we have the factorization

$$P(x) - P(\alpha) \;=\; (x-\alpha)Q(x)$$

Thus if $P(\alpha) = 0$ we have

$$P(x) \;=\; (x-\alpha)Q(x)$$

with $Q(x)$ a polynomial in $\mathcal{F}[x]$ of degree $n-1$. This enables us to prove the assertion by induction on $n$. Indeed, for $n = 1$ this relation clearly shows that $P(x)$ can have at most 1 root in $\mathcal{F}$. But then if we inductively assume the Lemma to be true up to $n-1$ then the same relation yields that $Q(x)$ cannot have more than $n-1$ roots and thus $P(x)$ itself cannot have more than $n$ roots completing the induction and the proof.

## Lemma 1.3

*In any field $\mathcal{F}$ of order $> n$ a polynomial $P(x) = c_0 + c_1 x + \cdots + c_n x^n \in \mathcal{F}[x]$ statisfies*

$$P(\beta) = 0 \qquad (\textit{for all } \beta \in \mathcal{F})$$

*if and only if*

$$c_0 = c_1 = \cdots = c_n = 0.$$

## Proof

Since the "*if*" part is trivial we need only prove that the vanishing of $P$ implies the vanishing of its coefficients. To this end note that by hypothesis $\mathcal{F}$ has at least $n+1$ distinct elements

$$\beta_1, \beta_2, \ldots, \beta_{n+1}\,.$$

Evaluating $P$ at these elements we get a system of equations

$$\begin{array}{rcl} c_0 + c_1\beta_1 + \cdots + c_n\beta_1^n &=& 0 \\ c_0 + c_1\beta_2 + \cdots + c_n\beta_2^n &=& 0 \\ \cdots\quad\cdots\quad\cdots\quad\cdots\quad\cdots\quad\cdots & & \\ c_0 + c_1\beta_{n+1} + \cdots + c_n\beta_1^n &=& 0 \end{array}$$

with determinant

$$\prod_{1\le i<j\le n+1} (\beta_i - \beta_j) \neq 0.$$

This forces the vanishing of the coefficients $c_0, c_1, \ldots, c_n$ and completes our proof.

Recall that a polynomial $P(x) \in \mathcal{F}[x]$ of positive degree is said to be "*irreducible*" in $\mathcal{F}$ if we cannot find two polynomials $R(x), S(x) \in \mathcal{F}[x]$ of degrees $> 0$ yielding the factorization

$$P(x) \;=\; R(x)S(x)$$

**Proposition 1.1**

*Let $A_1(x), A_2(x), \ldots, A_k(x), \in \mathcal{F}[x]$ and let $P(x) \in \mathcal{F}[x]$ irreducible in $\mathcal{F}$. If $P(x)$ divides the product*

$$A_1(x)A_2(x)\cdots A_k(x)$$

*then it must necessarily divide at least one of the the factors.*

**Proof**

Clearly there is nothing to prove if $k = 1$. So, proceeding by induction on $k$, let us assume the assertion valid up to $k-1$. To prove it for $k$, for convenience set

$$A(x) = A_1(x)\,, \qquad B(x) \;=\; A_2(x)\cdots A_k(x)\,.$$

We need only to show that if $P(x)$ divides $A(x)B(x)$ and doesn't divide $A(x)$ then it must divide $B(x)$. This done the inductive hypothesis will yield the result for $k$. This given, suppose if possible that $P(x)$ doesnot divide $A(x)$ nor $B(x)$. Now note that the irreduciblility of $P(x)$ forces the greatest common divisor of $P$ and $A$ to be either $P$ itself or a scalar. The same holds true for $P$ and $B$. Thus if $P$ doesn't divide $A$ nor $B$ it follows from the equation in 1.4 of the Berlekamp algorithm that we can construct four polynomials $h_a, k_a, h_b, k_b \in \mathcal{F}[x]$ yielding the identities

$$1 \;=\; h_a(x)A(x) + k_a(x)P(x)\,, \qquad 1 \;=\; h_b(x)B(x) + k_b(x)P(x)$$

But then multiplication of both sides gives

$$1 \;=\; h_a(x)h_b(x)A(x)B(x) \;+\; h_a(x)k_b(x)A(x)P(x) \;+\; k_a(x)h_b(x)P(x)B(x) \;+\; k_a(x)k_b(x)P(x)P(x)$$

and the assumption that $P(x)$ divides the product $A(x)B(x)$ immediately leads to a contradiction. This contradiction proves that if $P(x)$ doesn't divide $A(x)$ then it must divide $B(x)$ and our argument is complete.

This result has the following important corollary

## Theorem 1.1

*Every monic (†) polynomial $P(x) \in \mathcal{F}[x]$ has a unique factorization of the form*

$$P \;=\; \phi_1^{p_1}\phi_2^{p_2}\cdots\phi_k^{p_k} \tag{1.14}$$

*with $\phi_1, \phi_2, \ldots, \phi_k \in \mathcal{F}[x]$ distict, irreducible monic polynomials in $\mathcal{F}[x]$*

## Proof

(†) *Its leading coefficient is equal to* 1

Note that if $P$ is irreducible there is nothing to prove. On the other hand if $P(x)$ is not irreducible then it must have a factorization of the form $P(x) = A(x)B(x)$ with $degree(A) > 0$ and $degree(B) > 0$ and $A(x), B(x)$ monic polynomials in $\mathcal{F}[x]$ . But then the identity $degree(A) + degree(B) = degree(P)$ forces the inequalities

$$degree(A) < degree(P)\,, \qquad degree(B) < degree(P)$$

applying the same reasoning on $A(x)$ and $B(x)$ and then to their factors, and then to the factors of their factors..., we can easily see that, (since the degrees decrease at each step), we will necessarily reach a factorization of the form

$$P(x) \;=\; A_1(x)A_2(x)\dots A_n(x)$$

where each of the factors $A_i(x)$ is monic and irreducible in $\mathcal{F}[x]$. This proves existence since 1.14 can then be obtained by grouping together identical factors.

To show uniqueness, suppose if possible that we have

$$P \;=\; A_1(x)A_2(x)\dots A_n(x) \qquad \text{and} \qquad P \;=\; B_1(x)B_2(x)\dots B_m(x) \tag{1.15}$$

with all the $A_i(x)$ and $B_j(x)$ monic, irreducible polynomials in $\mathcal{F}[x]$.

This given, we can immediately derive from these equalities that $A_1$must be equal to one of the $B_j$. Indeed, from Proposition 1.1 and the irreducibility of $A_1$ and $B_1$, it follows that $A_1$ must be equal to $B_1$ or divide the product

$$B_2(x)B_3(x)\dots B_m(x)$$

If $A_1 \neq B_1$ then the same reasoning will give that $A_1 = B_2$ or divide the product

$$B_3(x)\dots B_m(x)$$

Clearly, proceeding in this manner we will necessarily find that $A_i = B_j$ for some $1 \leq j \leq m$. Thus, by relabeling the $B_j$, there is no loss in assuming that $A_1 = B_1$. This then yields the identity

$$A_2(x)\dots A_n(x) \;=\; B_2(x)\dots B_m(x)$$

It is easy to see that repeating this process we will eventually show that we must have $n = m$ and that infact the two original factorizations in 1.15 where none other than one a permutation of the other. This proves uniqueness and completes our proof.

## Remark 1.2

Note that if $f(x) \in \mathbb{F}_p[x]$ is a monic irreducible polynomial of degree $k$ in $\mathbb{F}_p[x]$, then the collection of polynomials

$$\Omega_{f(x)} \;=\; \left\{c_0 + c_1x + \cdots + c_{k-1}x^{k-1} \;:\; c_i \in \mathbb{F}_p \right\}$$

form a field of order $p^k$. Here addition is ordinary addition of polynomials in $\mathbb{F}_p[x]$ , multiplication is carried out "*mod* $f(x)$" by the Division Algorithm and inverses are computed by means of the star identity 1.4 of the Euclidean Algorithm. We shall here and after denote this field

$$\mathbb{F}_p[x]/(f(x))$$

and will refer to it as the "*quotient field of* $f(x)$". Our ultimate goal is to show that every finite field may obtained by this construction and that for any integer $k \geq 1$ all quotient fields obtained from an irreducible polynomials of degree $k$ are isomorphic.

### 1.3 Cyclotomic Polynomials

We recall that the Mœbius function is defined by setting for any integer $m$

$$\mu(m) \;=\; \begin{cases} (-1)^k & \text{if } m \text{ is a product of } k \text{ distinct primes, and} \\ 0 & \text{otherwise.} \end{cases} \tag{1.16}$$

For instance the following table gives first ten values of $\mu$

| $m$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $\mu$ | 1 | −1 | −1 | 0 | −1 | 1 | −1 | 0 | 0 | 1 |

It is customary to define a partial order on the natural numbers by setting $d \preceq n$ if and only if $d$ divides $n$. Sometimes the symbol "|" is used instead of " $\preceq$ ".

The following basic identity is at the root of many uses of the Moebius function.

## Proposition 1.2

*For any two integers $d \preceq n$ we have*

$$\sum_{d \preceq m \preceq n} \mu(\frac{n}{m}) \;=\; \begin{cases} 1 & \text{if } d = n \text{ , and} \\ 0 & \text{otherwise} \end{cases} \tag{1.17}$$

## Proof

Note that if $d \preceq m \preceq n$ then we can write $m = dm'$ and $n = dn'$. This allows us to cancel the common factor $d$ and derive that 1.17 is equivalent to

$$\sum_{1 \preceq m' \preceq n'} \mu(\frac{n'}{m'}) \;=\; \begin{cases} 1 & \text{if } n' = 1 \text{ , and} \\ 0 & \text{otherwise} \end{cases} \tag{1.18}$$

Clearly, when $d = n$ then $n' = 1$ and this sum reduces to the single term $\mu(1) = 1$. This gives the first case of 1.17. On the other hand when $d$ is strictly less than $n$, then in 1.18 $n'/m'$ runs over all divisors of $n'$. In other words we may as well rewrite 1.18 in the form

$$\sum_{1 \preceq m' \preceq n'} \mu(m') \;=\; \begin{cases} 1 & \text{if } n' = 1 \text{ , and} \\ 0 & \text{otherwise} \end{cases} \tag{1.19}$$

Now from the definition in 1.16 it follows that if $n' = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ then the only terms contributing to the sum in 1.19 are those where for some subset $S \subseteq \{1, 2, \ldots, k\}$ we have

$$m' \;=\; \prod_{i \in S} p_i$$

in which case $\mu(m') = (-1)^{|S|}$. Thus we are reduced to showing that

$$\sum_{S \subseteq \{1,2,\ldots,k\}} (-1)^{|S|} \;=\; 0\,. \tag{1.20}$$

But this is immediate since in 1.20 the terms equal to 1 and those equal to $-1$ are equal in number. For instance, a bijection yielding this equality is given by the involution $\phi$ on subsets of $\{1, 2, \dots, k\}$ obtained by letting $\phi(S) = S - \{1\}$ if $1 \in S$ and $\phi(S) = S + \{1\}$ if $1 \notin S$. This completes our argument.

This brings us the following important corollary of Proposition 1.2.

## Theorem 1.1

*Two sequences of numbers $\{A_n\}_{n\geq 1}$ and $\{B_n\}_{n\geq 1}$ are related by the equations*

$$B_n \;=\; \sum_{d \preceq n} A_d \qquad\qquad (\ \forall\ n \geq 1\ )\ , \tag{1.21}$$

*if and only if*

$$A_n \;=\; \sum_{m \preceq n} B_m\ \mu(\frac{n}{m}) \qquad\qquad (\ \forall\ n \geq 1\ )\ . \tag{1.22}$$

## Proof

Note that if we set $B_m = \sum_{d \preceq m} A_d$ in the right hand side of 1.22 it becomes

$$\sum_{m \preceq n}\ \Big(\ \sum_{d \preceq m} A_d\ \Big)\ \ \mu(\frac{n}{m})\ .$$

Changing order of summation this can be rewritten as

$$\sum_{d} A_d\ \Big(\ \sum_{d \preceq m \preceq n}\ \mu(\frac{n}{m})\ \Big)$$

and 1.22 immediately follows from 1.17.

Conversely, using 1.22, the right hand side of 1.21 becomes

$$\sum_{d \preceq n}\ \sum_{m \preceq d} B_m\ \mu(\frac{d}{m}) \;=\; \sum_{m} B_m \sum_{d}\ \ \mu(\frac{d}{m})\chi(m \preceq d \preceq n) \tag{1.23}$$

Now for a fixed $m$ and $n$ we have $m \preceq d \preceq n$ if and only if $d = d'm$ and $n = n'm$ thus

$$\sum_{d}\ \ \mu(\frac{d}{m})\chi(m \preceq d \preceq n) \;=\; \sum_{d'}\ \ \mu(d')\chi(1 \preceq d' \preceq n')$$

and 1.19 gives

$$\sum_{d}\ \ \mu(\frac{d}{m})\chi(m \preceq d \preceq n) \;=\; \begin{cases} 1 & \text{if } m = n \\ 0 & \text{otherwise} \end{cases}$$

Using this in 1.23 gives 1.21 and completes our proof.

Another important ingredient in the study of finite fields is the so called *Euler $\Phi$-function*. This is the function $\Phi(n)$ which gives the number of integers in the interval $[1, n]$ that have no factor in common with $n$. In symbols, we may define $\Phi(n)$ by setting

$$\Phi(n) \;=\; \#\{\ m \in [1, n]\ :\ (m, n) = 1\ \}\,. \tag{1.24}$$

It develops that $\Phi(n)$ has a most useful explicit formula.

## Theorem 1.2

*For an integer with prime factorization*

$$n \;=\; p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

*we have*

$$\Phi(n) \;=\; n\,(1-\tfrac{1}{p_1})(1-\tfrac{1}{p_2})\cdots(1-\tfrac{1}{p_k}) \tag{1.25}$$

*as well as*

$$\Phi(n) \;=\; \sum_{d \preceq n} \mu(d)\,\frac{n}{d} \tag{1.26}$$

## Proof

The best way to prove 1.25 is to use the "*principle of inclusion exclusion*" since by this path we gain one more tool for future use. The general set up is as follows. We have a finite set $\Omega$ and we are given certain subsets $A_1, A_2, \ldots, A_k \subseteq \Omega$. We are asked to count the number $N$ of elements of $\Omega$ that do not belong to any of these subsets. Setting

$$\chi_{A_i}(x) \;=\; \begin{cases} 1 & \text{if } x \in A_i \\ \\ 0 & \text{otherwise} \end{cases},$$

this number $N$ is simply given by the expression

$$N \;=\; \sum_{x\in\Omega} \prod_{i=1}^{k} \big(1-\chi_{A_i}(x)\big). \tag{1.27}$$

Since

$$\prod_{i=1}^{k} \big(1-\chi_{A_i}(x)\big) \;=\; \sum_{S\subseteq[1,k]} (-1)^{|S|} \prod_{i\in S} \chi_{A_i}(x),$$

using this in 1.27 gives

$$\begin{aligned} N \;&=\; \sum_{S\subseteq[1,k]} (-1)^{|S|} \sum_{x\in\Omega} \prod_{i\in S} \chi_{A_i}(x) \\ &=\; \sum_{S\subseteq[1,k]} (-1)^{|S|}\, \#\bigcap_{i\in S} A_i\,. \end{aligned} \tag{1.28}$$

Getting back to the proof of our theorem, if we let $\Omega$ be the set of integers in the interval $[1,n]$ and $A_i$ be the subset of these integers that are divisible by $p_i$, then we can easily see that, with these choices, our $\Phi(n)$ is none other than the $N$ in 1.27. To apply 1.28 we simply note that if $S = \{i_1, i_2, \ldots, i_s\}$ then, $\bigcap_{i\in S} A_i$ reduces to the subset of integers in $[1,n]$ that are divisible by the product $p_{i_1} p_{i_2} \cdots p_{i_s}$. Thus in this case, we have

$$\#\bigcap_{i\in S} A_i \;=\; \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_s}}$$

Using this in 1.28 we finally derive that

$$\Phi(n) \;=\; \sum_{s=0}^{n} \sum_{1\le i_1<i_2<\cdots<i_s\le n} (-1)^s\, \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_s}} \tag{1.29}$$

and it is easily seen that this simply another way of writing 1.25. Moreover, since $\mu(p_{i_1}p_{i_2}\cdots p_{i_s}) = (-1)^s$ we see that 1.29 is also another way of writing 1.26. This completes our proof.

Recall that an element $\alpha$ of a Group $G$ is said to be "*an $n^{th}$ root of unity*" if $\alpha^n = 1$ we shall also say that $\alpha$ is of "*order $k$*" and write "$ord(\alpha) = k$", if and only if

$$\alpha^k = 1 \quad \text{and} \quad \alpha^s \neq 1 \quad \text{for } 1 \leq s \leq k-1$$

There are four important properties of the notion of order which play an important role in our developments and are good to keep in mind.

## Proposition 1.3

*In a multiplicative group $G$*

*(1) If an element $\alpha \in G$ has order $n$ then $\alpha^m = 1$ if and only if $n$ divides $m$.*

*(2) If an element $\alpha \in G$ has order $n$ then the element $\alpha^k$ has order $\frac{n}{(n,k)}$*

*(3) If $\alpha, \beta \in G$ have orders $a$ and $b$ respectively and $(a,b) = 1$ then $\alpha\beta$ has order $ab$.*

*(4) If $n$ is the maximal order of any element of $G$ then the order of any other element of $G$ is a divisor of $n$.*

## Proof

Note that if $ord(\alpha) = n$ and $\alpha^m = 1$ then of course we must have $m \geq n$ and if $m > n$ then by division we get $m = nQ + R$ with $0 \leq R < n$ but then

$$\alpha^m = \alpha^{nQ+R} = \alpha^R = 1$$

and $R > 0$ contradicts the nature of $n$. This proves (1). Now again if $ord(\alpha) = n$ then we see that

$$(\alpha^k)^{\frac{n}{(n,k)}} \;=\; (\alpha^n)^{\frac{k}{(n,k)}} \;=\; 1.$$

On the other hand if $(\alpha^k)^m = 1$ then from (1) it follows that $n$ divides $km$ so suppose that for some integer $r$ we have $km = r\,n$. But we must also have

$$\tfrac{k}{(n,k)}\; m \;=\; r\,\tfrac{n}{(n,k)}$$

and since $\frac{k}{(n,k)}$ and $\frac{n}{(n,k)}$ are relatively prime it follows from this that $\frac{n}{(n,k)}$ must divide $m$. This proves (2). To prove (3) note that

$$(\alpha\beta)^m = 1 \quad \rightarrow \quad \alpha^m = \beta^{-m} \quad \text{and} \quad \beta^m = \alpha^{-m}$$

thus we also have

$$\alpha^{mb} = 1 \quad \text{and} \quad \beta^{ma} = 1$$

and (1) together with $ord(\alpha) = a$ and $ord(\beta) = b$ give that

$$a|mb \quad \text{and} \quad b|ma$$

but now the hypothesis that $(a,b) = 1$ forces $m$ to be divisible by the product $ab$. Since we clearly have

$$(\alpha\beta)^{ab} \;=\; (\alpha^a)^b(\beta^b)^a \;=\; 1$$

our proof of (3) is now complete.

Finally, suppose that $\alpha \in G$ has order $n$ and every other element of $G$ has order $\leq n$. Suppose if possible that some element $\beta \in G$ has order $m$ and that $m$ does not divide $n$. Then there will be some prime factor $p$ of $m$ with the property that $p^e$ (for some $e \geq 1$) divides $m$ and $p^{e-1}$ is the maximal power of $p$ that divides $n$. Now from (2) it follows that

$$ord\big(\alpha^{p^{e-1}}\big) = \frac{n}{p^{e-1}} \quad \text{and} \quad ord\big(\beta^{\frac{m}{p^e}}\big) = p^e$$

since $\frac{n}{p^{e-1}}$ and $p^e$ are relatively prime it follows from (3) that

$$ord\big(\alpha^{p^{e-1}}\,\beta^{\frac{m}{p^e}}\big) \;=\; n\,p$$

and that contradicts that $n$ is the largest order of any element of $G$. This completes our proof.

Now for some integer $n > 1$, set $\omega = e^{2\pi i/n}$ and note that the n complex numbers

$$1, \omega, \omega^2, \ldots, \omega^{n-1} \tag{1.30}$$

are all solutions of the equation $t^n - 1 = 0$ and since they are distinct and the polynomial $1 - t^n$ has at most $n$ roots it follows that we must have

$$t^n - 1 \;=\; \prod_{i=0}^{n-1}(t - \omega^i). \tag{1.31}$$

Note further that if $d$ is a divisor of $n$ then by (1) of Proposition 1.3 it follows that every complex number $\beta$ of order $d$ must be a root of the polynomial $t^n - 1$ and therefore must be one of the elements in 1.30. Thus if we set

$$Q_d(t) \;=\; \prod_{\substack{ord(\beta)=d \\ \beta\in\mathbb{C}}} (t - \beta) \tag{1.32}$$

then, we must necessarily have the factorization

$$t^n - 1 \;=\; \prod_{d|n} Q_d(t) \tag{1.33}$$

The expression in 1.32 defines the so called "$d^{th}$ *cyclotomic polynomial* ". As we shall see this polynomial has remarkable properties and plays a basic role in every field. To begin it can be given an explicit formula.

## Theorem 1.4

*For all $d > 1$ we have*

$$Q_m(t) \;=\; \prod_{n|m}(t^n - 1)^{\mu(m/n)} \tag{1.34}$$

*In particular $Q_m(t)$ is always a monic polynomial with integer coefficients.*

## Proof

Note that using 1.33 in the right hand side of 1.34 we get

$$\begin{aligned} RHS &= \prod_{n|m}\prod_{d|n} Q_d(t)^{\mu(m/n)} \\ &= \prod_{d} Q_d(t)^{\sum_{d \preceq n \preceq m}\mu(m/n)} \end{aligned}$$

and 1.34 follows by another use of 1.17. This given, we can write 1.34 in the form

$$Q_m(t) \prod_{\substack{n|m \\ \mu(m/n)=-1}} (t^n-1) = \prod_{\substack{n|m \\ \mu(m/n)=1}} (t^n-1). \tag{1.35}$$

Now both products on the right and on the left of this equality are clearly monic polynomials with integer coefficients. We thus deduce from 1.35, by the division algorithm, that $Q_m(t)$ must be a monic polynomial with rational coefficients and thus the last assertion is an immediate consequence of Gauss lemma. This completes our proof.

Formula 1.34 gives a practical way to compute a given cyclotomic polynomial. For instance, when $n = 6$ from the following table

| $n$ | 1 | 2 | 3 | 6 |
|---|---|---|---|---|
| $\frac{m}{n}$ | 6 | 3 | 2 | 1 |
| $\mu(\frac{m}{n})$ | 1 | $-1$ | $-1$ | 1 |
| $x^n-1$ | $x-1$ | $x^2-1$ | $x^3-1$ | $x^6-1$ |

we get

$$Q_6(x) = \frac{(x-1)(1-x^6)}{(x^2-1)(x^3-1)} = \frac{(x^3+1)}{(x+1)} = 1-x+x^2 \ .$$

We give below a list of the polynomials $Q_{p-1}(x)$ as $p$ runs over the first 14 primes.

$$\begin{aligned} Q_1(x) &= x-1 \\ Q_2(x) &= 1+x \\ Q_4(x) &= 1+x^2 \\ Q_6(x) &= 1-x+x^2 \\ Q_{10}(x) &= 1-x+x^2-x^3+x^4 \\ Q_{12}(x) &= 1-x^2+x^4 \\ Q_{16}(x) &= 1+x^8 \\ Q_{18}(x) &= 1-x^3+x^6 \\ Q_{22}(x) &= 1-x+x^2-x^3+x^4-x^5+x^6-x^7+x^8-x^9+x^{10} \\ Q_{28}(x) &= 1-x^2+x^4-x^6+x^8-x^{10}+x^{12} \\ Q_{30}(x) &= 1+x-x^3-x^4-x^5+x^7+x^8 \\ Q_{36}(x) &= 1-x^6+x^{12} \\ Q_{40}(x) &= 1-x^4+x^8-x^{12}+x^{16} \\ Q_{42}(x) &= 1+x-x^3-x^4+x^6-x^8-x^9+x^{11}+x^{12} \end{aligned}$$

We should point out the following important relation between the Euler $\Phi$-function and the cyclotomic polynomials.

## Proposition 1.4

$$degree\ Q_m(x) \ = \ \Phi(m) \tag{1.36}$$

*In particular 1.33 gives*

$$\sum_{d \preceq n} \Phi(d) \ = \ n \tag{1.37}$$

## Proof

From 1.35 it follows that the degree of the polynomial $Q_n(x)$ may be computed by subtracting the degree of the product on the left from the degree of the product on the right. This gives

$$degree\ Q_m(x) \ = \ \sum_{\substack{n|m \\ \mu(m/n)=1}} n \ - \ \prod_{\substack{n|m \\ \mu(m/n)=-1}} n \ = \ \sum_{n \preceq m} n\, \mu(\frac{m}{n}) \ .$$

Thus 1.36 follows from the identity in 1.26. We also see from formula 1.33 that $n$, which is the degree of $1-x^n$, must also be equal to the sum of the degrees of the factors $\phi_d(x)$ as $d$ varies over the divisors of $n$. This establishes 1.37 and completes our proof.

In a finite field $\mathcal{F}$ of order $q$ an element $\alpha$ is said to be "*primitive* " if and only if

$$\begin{aligned} &(i) \quad \alpha^{q-1} = 1 \quad \text{and} \\ &(ii) \quad \{\alpha, \alpha^2, \ldots, \alpha^{q-1}\} \ = \ \mathcal{F} - \{0\} \end{aligned} \tag{1.38}$$

Note all this says, in this case, is that $ord(\alpha) = q-1$.

Proposition 1.3 and 1.4 combined have the following surprising corollary.

## Theorem 1.5

*A finite field $\mathcal{F}$ of order $q$ has exactly $\Phi_{q-1}$ primitive elements. In fact, for any $d \preceq q-1$ the cyclotomic polynomial $Q_d(t)$ has exactly $\Phi(d)$ roots in $\mathcal{F}$ and they constitute all the elements of order $d$ in $\mathcal{F}$.*

## Proof

Since $\mathcal{F}$ has order $q < \infty$ every non-zero element $\beta \in \mathcal{F}$ has an order bounded by $q-1$. Note that if we set

$$n_o \ = \ \max\{ord(\beta) \,:\, \beta \in \mathcal{F}\}$$

then from (4) of Proposition 1.3 it follows that in the multiplicative group $\mathcal{F}-\{0\}$ the order of every element must divide $n_o$. But that means that the elements of $\mathcal{F} - \{0\}$ are all roots of the equation

$$x^{n_o} - 1 = 0\,.$$

Since from Lemma 1.2 this equation cannot have more than $n_o$ roots it follows that

$$\#\big(\mathcal{F} - \{0\}\big) \le n_o$$

This gives

$$q-1 \leq n_o. \tag{1.39}$$

On the other hand if $\alpha$ has order $n_o$ then the elements

$$1, \alpha, \alpha^2, \ldots, \alpha^{n_o-1} \tag{1.40}$$

are distict and since they are all in $\mathcal{F}-\{0\}$ we must necessarily also have

$$n_o \leq q-1.$$

This together with 1.39 proves the equality

$$n_o = q-1$$

and from the definition in 1.38 it follows that $\alpha$ is a primitive element of $\mathcal{F}$. Moreover this equality now yields the following three basic facts

(1) *Every non-zero element of $\mathcal{F}$ must have an order that is a divisor of $q-1$*
(2) *Every non-zero element of $\mathcal{F}$ must be one of the elements in 1.40*
(3) *Every non-zero element of $\mathcal{F}$ must be a root of the polynomial $x^{q-1}-1$*

Note that since $x^{q-1}-1$ has no more than $q-1$ roots it follows from (2) and (3) that

$$x^{q-1}-1 \;=\; \prod_{\beta\in\mathcal{F}-\{0\}}(x-\beta) \;=\; \prod_{i=0}^{q-2}(x-\alpha^i) \tag{1.41}$$

But now (1) combined with the first equality in 1.41 yields that we must have

$$x^{q-1}-1 \;=\; \prod_{d\,\preceq\,q-1}\;\prod_{\substack{\beta\in\mathcal{F}-\{0\}\\ ord(\beta)=d}}(x-\beta). \tag{1.42}$$

Now fix $n \preceq q-1$ and set $\gamma=\alpha^{\frac{q-1}{n}}$. By (2) of Proposition 1.3 it follows that $ord(\gamma)=n$, and the thus the elements

$$1, \gamma, \gamma^2, \ldots, \gamma^{n-1}$$

are distinct and satisfy the equation $x^n-1=0$. Since this equation cannot have more than $n$ solutions in $\mathcal{F}$, it follows that these elements are all the $n^{th}$ roots of unity of $\mathcal{F}$. Thus we must have the two factorizations

$$x^n-1 \;=\; \prod_{i=0}^{n-1}(x-\gamma^i) \;=\; \prod_{\substack{\beta\in\mathcal{F}-\{0\}\\ \beta^n=1}}(x-\beta).$$

grouping the factors of the last product according to the order of the corresponding element we derive that for any $n \preceq q-1$ we must also have

$$x^n-1 \;=\; \prod_{d\,\preceq\,n}\;\prod_{\substack{\beta\in\mathcal{F}-\{0\}\\ ord(\beta)=d}}(x-\beta). \tag{1.43}$$

Setting for a moment

$$R_d(x) \;=\; \prod_{\substack{\beta\in\mathcal{F}-\{0\}\\ ord(\beta)=d}} (x-\beta)$$

1.43 becomes

$$x^n-1 \;=\; \prod_{d\,\preceq\, n} R_d(x) \qquad (\text{for all } n\;\preceq\; q-1)$$

Thus for any $m\;\preceq\; q-1$ we have

$$\begin{aligned}\prod_{n\,\preceq\, m}(x^n-1)^{\mu(\frac{m}{n})} \;&=\; \prod_{n\,\preceq\, m}\;\prod_{d\,\preceq\, n}\big(R_d(x)\big)^{\mu(\frac{m}{n})}\\ &=\; \prod_{d}\big(R_d(x)\big)^{\sum_{d\,\preceq\, n\,\preceq\, m}\mu(\frac{m}{n})}\\ (\text{by 1.17}) \;&=\; R_m(x)\end{aligned}$$

and 1.34 gives

$$R_m(x) \;=\; Q_m(x)$$

Thus the factorization in 1.42 is none other than

$$x^{q-1}-1 \;=\; \prod_{d\,\preceq\, q-1} Q_d(x) \tag{1.44}$$

Now note that the polynomial $1-x^{q-1}$ has $q-1$ roots given by the elements

$$1,\alpha,\alpha^2,\ldots,\alpha^{q-2} \tag{1.45}$$

moreover 1.37 for $n=q-1$ gives

$$\sum_{d\,\preceq\, q-1}\Phi(d) \;=\; q-1$$

Thus from 1.44, 1.36 and Lemma 1.2 it follows that for $d\;\preceq\; q-1$ each polynomial $Q_d(x)$ has precisely $\Phi(d)$ roots in $\mathcal{F}$ and these roots are all the elements of order $d$ in $\mathcal{F}$. This proves the last assertion of the Theorem. In particular we derive that $\mathcal{F}$ contains exactly $\Phi_{q-1}$ elements of order $q-1$ which a fortiori must be all the primitive roots of $\mathcal{F}$. This completes our proof.

We should note that the proof of Theorem 1.5 yields also the following interesting fact.

## Proposition 1.5

*If $\alpha$ is any primitive root of $\mathcal{F}$ then the set of elements*

$$\mathcal{P} \;=\; \{\alpha^k\,:\,(k,q-1)=1\}$$

*gives all the primitive roots of $\mathcal{F}$. In particular we also have*

$$Q_{q-1}(x) \;=\; \prod_{\substack{1\le k\le q-1\\ (k,q-1)=1}}\big(x-\alpha^k\big) \tag{1.46}$$

## Proof

It follows from (2) of Proposition 1.3 that all the elements of $\mathcal{P}$ have order $q-1$. On the other hand the definition in 1.24 of the Euler $\Phi$-function gives that the set $\mathcal{P}$ has cardinality precisely $\Phi(q-1)$ but the latter is, in fact, also the degree of $Q_{q-1}(x)$ whose roots are all the primitive elements of $\mathcal{F}$. This proves the Theorem (including 1.46).

## Problems

1. Since it follows from the Euclidean algorithm that the integers modulo a prime $p$ form a field $\mathbb{F}_p$ . We can use Theorem 1.4 to determine the primitive roots of $\mathbb{F}_p$ for any prime $p$. Test your understanding of the material in this subsection by constructing all the primitive roots of $\mathbb{F}_{19}$.
2. Use the results of problem **1.** to construct the inverse of 15 in $\mathbb{F}_{19}$ without using the Euclidean algorithm.

## 1.4 The Frobenius map

In a finite field $\mathcal{F}$ of characteristic $p$ the map $\phi : \mathcal{F}\to\mathcal{F}$ obtained by setting

$$\phi(\beta) \;=\; \beta^p \qquad (\text{for all } \beta\in\mathcal{F}) \tag{1.47}$$

is usually referred to as the "*Frobenius map*". As we shall soon see, this map has a variety of truly remarkable properties, but before we can present them we need some auxiliary facts. To begin we shall assume, here and after, whether explicitly stated or not, that our field $\mathcal{F}$ has characteristic $p$.

## Proposition 1.6

*For any elements $a_1, a_2, \dots a_n \in \mathcal{F}$ and any integer $k > 0$ we have*

$$(a_1 + a_2 + \cdots + a_n)^{p^k} \;=\; a_1^{p^k} + a_2^{p^k} + \cdots + a_n^{p^k} \tag{1.48}$$

## Proof

To begin note that the binomial coefficient $\binom{p}{k}$ necessarily vanishes in $\mathcal{F}$ for any $r = 1, 2 \dots, p-1$. Indeed we see that, $p$ being a prime, for these values of $r$, the factors in the denominators in the formula

$$\binom{p}{r} \;=\; \frac{p!}{r!(p-r)!}$$

cannot cancel the factor $p$ contained in $p!$. This given, the identity

$$(a_1 + a_2)^p \;=\; \sum_{r=0}^{p} \tbinom{p}{r} a_1^r a_2^{p-r}$$

reduces to

$$(a_1 + a_2)^p \;=\; a_1^p + a_2^p \qquad (\text{in } \mathcal{F})$$

This proves 1.48 for $n = 2$ and $k = 1$. To prove the general case assume by induction that 1.48 is true for $k = 1$ and $n-1$. But then the $n = 2$ case and the inductive hypothesis gives

$$(a_1 + a_2 + \cdots + a_n)^p \;=\; a_1^p \;+\; (a_2 + \cdots + a_n)^p \;=\; a_1^p + a_2^p + \cdots + a_n^p$$

This completes the induction and proves 1.48 for $k = 1$. Next note that a double use of $k = 1$ case identity gives

$$(a_1 + a_2 + \cdots + a_n)^{p^2} \;=\; (a_1^p + a_2^p + \cdots + a_n^p)^p \;=\; a_1^{p^2} + a_2^{p^2} + \cdots + a_n^{p^2}$$

and we can easily see that what remains to be proved follows again by an inductive argument.

This identity has an immediate important corollary.

## Proposition 1.7

*In a field $\mathcal{F}$ of characteristic $p$ no element can have an order that is divisible by $p$.*

## Proof

Suppose that for some element $\beta \in \mathcal{F}$ we have

$$\beta^{mp} \;=\; 1$$

Then since 1.48 gives

$$(\beta^m - 1)^p \;=\; \beta^{mp} \;+\; (-1)^p \;=\; \beta^{mp} \,-\, 1 \;^{(\dagger)}$$

we must also have

$$\beta^m \;=\; 1$$

Thus $mp$ cannot possibly be the order of $\beta$. This completes our argument.

## Proposition 1.8

*An element $\alpha \in \mathcal{F}$ belongs to the subfield $\mathbb{F}_p$ if and only if*

$$\alpha^p \;=\; \alpha \tag{1.49}$$

*In other words under the Frobenius map the only elements of $\mathcal{F}$ that remain fixed are those in $\mathbb{F}_p$.*

## Proof

Note that since $\mathbb{F}_p$ has $p$ elements it follows from the proof of Theorem 1.5 that all the non-zero elements of $\mathbb{F}_p$ satisfy the polynomial equation

$$x^{p-1} - 1 \;=\; 0.$$

that means that $0, 1, \ldots, p-1$ satisfy the equation

$$x^p - x \;=\; 0$$

since the polynomial $x^p - x$ cannot have more than $p$ roots in $\mathcal{F}$, the elements of $\mathbb{F}_p$ must be the only ones in $\mathcal{F}$ that satisfy the condition in 1.49. This completes the proof.

We are now in a position to establish a most remarkable property of finite fields

$^{(\dagger)}$ This is also true when $p = 2$ since in characteristic 2 we have $1 = -1$

## Theorem 1.9

*In a finite field $\mathcal{F}$ of characteristic $p$ an element $\beta \in \mathcal{F}$ of order $d$ generates, under the action of the Frobenius map $\phi$, a cycle of length $m$, where $m$ is the order of $p$ in the integers $mod\ d$. That is the elements*

$$\beta\ ,\ \beta^p\ ,\ \beta^{p^2}, \dots\ ,\ \beta^{p^{m-1}} \tag{1.50}$$

*are distinct and we have*

$$\beta^{p^m} \ = \ \beta \tag{1.51}$$

*Thus, under $\phi$, $\mathcal{F}$ breaks up into the union of disjoint cycles. In other words the Frobenius map permutes the elements of $\mathcal{F}$ and therefore it is invertible in $\mathcal{F}$.*

## Proof

By definition, $m$ is the order of $p$ mod $d$ if and only if

$$a) \quad p^m \ = \ 1 \ (\text{mod } d) \quad \& \quad b) \quad p^s \neq 1 \pmod{d} \quad (\text{for } 1 \leq s \leq m-1) \tag{1.52}$$

Clearly, 1.52 a) gives 1.51. Moreover, if for some pair $i < j$ we have

$$\beta^{p^j} \ = \ \beta^{p^i}$$

then dividing both sides by $\beta^{p^i}$ we get

$$\beta^{p^i(p^{j-i}-1)} \ = \ 1.$$

In particular, $d$ must divide the product $p^i(p^{j-i}-1)$. Since by Proposition 1.7 $d$ cannot have $p$ as a factor, it follows that $d$ must divide $p^{j-i}-1$. In other words

$$p^{j-i} = 1 \qquad (mod\ d)$$

But from b) of 1.52 we see that this cannot happen when $1 \leq i < j \leq m-1$. Thus the elements in 1.50 are distinct, precisely as asserted, and 1.51 shows that these elements constitute a cycle of the Frobenius map. Since every element of $\mathcal{F}$ has a finite order and cycles that share an element are necessarily identical, the last two assertions are immediate.

## Proposition 1.9

*In a finite field $\mathcal{F}$ of order $q$, polynomial $P(x) \in \mathcal{F}[x]$ of degre $n < q$ satisfies the identity*

$$P(\beta)^p \ = \ P(\beta^p) \qquad (\textit{for all } \beta \in \mathcal{F}) \tag{1.53}$$

*if and only if*

$$P(x) \in \mathbb{F}_p[x].$$

## Proof

Let

$$P(x) = c_0 + c_1 x + \cdots + c_n x^n$$

We are to show that 1.53 holds if and only if

$$c_0 \in \mathbb{F}_p\ ,\quad c_1 \in \mathbb{F}_p\ ,\quad \dots\ ,\ c_n \in \mathbb{F}_p\ , \tag{1.54}$$

Note first that from 1.48 it follows that

$$P(\beta)^p \ = \ c_0^p + c_1^p\beta^p + \cdots + c_n^p\beta^{pn}.$$

Thus the condition in 1.53 is none other than

$$c_0^p + c_1^p\beta^p + \cdots + c_n^p\beta^{pn} \ = \ c_0 + c_1\beta^p + \cdots + c_n\beta^{pn} \tag{1.55}$$

that is we must have

$$Q(x) \ = \ c_0^p - c_0 \ + \ (c_1^p - c_1)\beta^p \ + \ \cdots + (c_n^p - c_n)\beta^{pn} \ = \ 0 \qquad (\text{for all } \beta \in \mathcal{F}) \tag{1.56}$$

Since by Theorem 1.9 the Frobenius map permutes the elements of $\mathcal{F}$ it follows that 1.56 is equivalent to the condition

$$Q(x) \ = \ c_0^p - c_0 \ + \ (c_1^p - c_1)\beta \ + \ \cdots + (c_n^p - c_n)\beta^n \ = \ 0 \qquad (\text{for all } \beta \in \mathcal{F})$$

However since $n < q$ we can use Lemma 1.3. and derive that

$$c_0^p = c_0\ ,\quad c_1^p = c_1\ ,\quad \dots\ ,\quad c_n^p = c_n \tag{1.57}$$

and 1.54 then follows from Proposition 1.8. Conversely, by the same Proposition the relations in 1.54 give 1.57 and 1.56 must hold true for all $\beta \in \mathcal{F}$ and we have seen that this is equivalent to 1.53. Thus our proof is complete.

This brings us to another basic result on finite fields.

## Theorem 1.10

*In a finite field $\mathcal{F}$ of order $q$ and characteristic $p$ an element $\beta$ of order $d$ is a root of a monic irreducible polynomial $\phi_\beta(x) \in \mathbb{F}_p[x]$ of degree equal to the order of $p$ in the integers mod $d$. In fact, we have*

$$\phi_\beta(x) \ = \ \prod_{s=0}^{m-1}(x - \beta^{p^s}) \tag{1.59}$$

*where $\beta, \beta^p, \cdots, \beta^{p^{m-1}}$ are none other than the elements of the Frobenius cycle generated by $\beta$. It then follows that $\beta$ generates within $\mathcal{F}$ a subfield of order $p^m$ that is isomorphic to the quotient field $\mathbb{F}_p[x]/(\phi_\beta(x))$ .*

## Proof

To prove the first assertion it suffices to show that the polynomial $\phi_\beta(x)$ defined by 1.59 lies in $\mathbb{F}_p[x]$ and is irreducible in $\mathbb{F}_p[x]$. To this end note first that since by Proposition 1.6 we have

$$(x - \beta^{p^s})^p \ = \ (x^p - \beta^{p^{s+1}})$$

we derive that

$$\phi_\beta(x)^p \;=\; \prod_{s=1}^{m}(x^p-\beta^{p^s}) \;=\; \phi_\beta(x^p)$$

since $m<q$ we can use Proposition 1.9 and derive that $\phi_\beta(x)\in\mathbb{F}_p[x]$. Next suppose that for two polynomials $A(x),B(x)\in\mathbb{F}_p[x]$ of degree $<m$ we have

$$A(x)B(x) \;=\; \phi_\beta(x)$$

then setting $x=\beta$ gives

$$A(\beta)B(\beta) \;=\; \phi_\beta(\beta) \;=\; 0.$$

Thus if $B(\beta)\neq 0$ we must have $A(\beta)=0$, but then from Proposition 1.9 we derive that

$$A(\beta)=A(\beta^p)=A(\beta^{p^2})=\cdots=A(\beta^{p^{m-1}}) \;=\; 0$$

but this yields a contradiction since a polynomial of degree $<m$ cannot have $m$ distinct roots. The same contradiction arises if we assume that $A(\beta)\neq 0$. This proves that $\phi_\beta(x)$ is irreducible in $\mathbb{F}_p[x]$.

Now note that the collection

$$\mathbb{F}_p[\beta] \;=\; \left\{c_0+c_1\beta+\cdots+c_{m-1}\beta^{m-1} \;:\; c_0,c_1,\ldots,c_{m-1}\in\mathbb{F}_p\right\}$$

consists of $p^m$ distinct elements. Indeed, the equality of any two of them yields a polynomial equation of degree less than $m$ satisfied by $\beta$, contradicting the irreducibility of $\phi_\beta(x)$. Furthermore, it is easily seen that $\mathbb{F}_p[\beta]$ is a subfield of $\mathcal{F}$ which is isomorphic to the quotient field $\mathbb{F}[x]/(\phi_\beta(x))$. In fact the isomorphism is simply given by the map

$$ev_\beta : \mathbb{F}[x]/(\phi_\beta(x)) \;\to\; \mathbb{F}_p[\beta]$$

obtained by setting

$$ev_\beta f(x) \;=\; f(\beta)\,.$$

This map is clearly onto and well defined since if for three elements $f(x),g(x),h(x)\in\mathbb{F}_p[x]$ we have

$$f(x) \;=\; g(x) \;+\; \phi_\beta(x)h(x)$$

then then setting $x=\beta$ gives

$$f(\beta) \;=\; g(\beta)\,.$$

It is also injective since if for some $f(x)\in\mathbb{F}_p[x]$ we have

$$f(\beta) \;=\; 0$$

then the irreducibility of $\phi_\beta(x)$ yields that $f(x)$ must be a multiple of $\phi_\beta(x)$. Likewise, $ev_\beta$ preserves multiplication since if for four elements $f(x),g(x),h(x),k(x)\in\mathbb{F}_p[x]$ we have

$$f(x)g(x) \;=\; h(x) \;+\; \phi_\beta(x)k(x).$$

then setting $x = \beta$ gives

$$f(\beta)g(\beta) \;=\; h(\beta)$$

Similarly if

$$f(x) + g(x) \;=\; h(x) \;+\; \phi_\beta(x)k(x).$$

then setting $x = \beta$ gives

$$f(\beta) + g(\beta) \;=\; h(\beta)$$

Thus $ev_\beta$ preserves addition as well and our proof is complete.

An immediate corollary of Theorem 1.10 yields the nature of a finite field.

## Theorem 1.11

*Let be a finite field $\mathcal{F}$ of characteristic $p$ and order $q$ then*

$$q = p^k \tag{1.58}$$

*where $k$ is the order of $p$ mod $q-1$. In fact, for any primitive element $\alpha \in \mathcal{F}$ we have the equality*

$$\mathbb{F}_p[\alpha] \;=\; \mathcal{F}. \tag{1.59}$$

## Proof

Theorem 1.5 gives that $\mathcal{F}$ has $\Phi_{q-1}$ primitive elements. Let $\alpha$ be one of them. From Theorem 1.10 it follows that $\alpha$ generates a subfield of

$$\mathbb{F}_p[\alpha] \subseteq \mathcal{F} \tag{1.60}$$

of order $p^k$ with $k$ the order of $p$ mod $q-1$. Thus

$$p^k \le q \tag{1.61}$$

On the other hand since we must have $p^k - 1 = 0$ modulo $q-1$ it follows that $q-1$ must divide $p^k - 1$. This gives

$$q - 1 \le p^k - 1 \tag{1.62}$$

and the equality in 1.58 immediately follows by combining 1.61 and 1.62. But now 1.58 together with 1.60 forces the equality in 1.59 and completes our proof.

Theorem 1.11 essentially states that every finite field of characteristic $p$ is isomorphic to a quotient field $\mathbb{F}_p[x]/(f(x))$ with $f(x)$ a monic polynomial irreducible in $\in \mathbb{F}_p[x]$. To get deeper into the nature of finite fields we need two auxiliary results.

## Lemma 1.3

*For any given prime $p$ and any two integers $1 \le h < k$ we have*

$$p^h - 1 \;\preceq\; p^k - 1 \qquad \Longleftrightarrow \qquad h \;\preceq\; k \tag{1.63}$$

## Proof

It easily verified that for any three integers $h, k, r$ we have

$$x^k - 1 \;=\; (x^h - 1)\big(1 + x^h + x^{2h} + \cdots + x^{(r-1)h}\big) \;+\; x^{rh}\big(x^{k-rh} - 1\big) \tag{1.65}$$

We shall use it here for $h < k$ and

$$r \;=\; \max\{i \,:\, k - ih \geq 0\}, \tag{1.66}$$

and note that we have

$$h \;\preceq\; k \qquad \Longleftrightarrow \qquad k - rh = 0 \tag{1.67}$$

Making the replacement $x \to p$ in 1.65 gives

$$p^k - 1 \;=\; (p^h - 1)\big(1 + p^h + p^{2h} + \cdots + p^{(r-1)h}\big) \;+\; p^{rh}\big(p^{k-rh} - 1\big)\,. \tag{1.68}$$

Note that if $h \;\preceq\; k$ then from 1.67 it follows that

$$p^k - 1 \;=\; (p^h - 1)\big(1 + p^h + p^{2h} + \cdots + p^{(r-1)h}\big),$$

which yields that $p^h - 1$ divides $p^k - 1$. This proves the left pointing arrow in 1.63. To prove the converse we need only show that $p^h - 1 \;\preceq\; p^k - 1$ forces $k - rh = 0$. To this end suppose if possible that $k - rh > 0$ and note that if $p^h - 1$ divides $p^k - 1$ then it follows from 1.68 that $p^h - 1$ must also divide $p^{rh}\big(p^{k-rh} - 1\big)$. Since $p^h - 1$ can't have any factor in common with $p^{rh}$ it must be that $p^h - 1$ divides $p^{k-rh} - 1$. Now this implies

$$p^h - 1 \leq p^{k-rh} - 1$$

or equivalently

$$h \leq k - rh.$$

But this is in plain contradiction with the definition of $r$ in 1.66. Thus only the alternative $k - rh = 0$ is compatible with $p^h - 1 \;\preceq\; p^k - 1$ and our proof is complete.

The equivalence in 1.63 has a most unexpected consequence.

## Theorem 1.12

*In a finite field $\mathcal{F}$ of order $p^k$ all the Frobenius cycles have lengths that divide $k$.*

## Proof

Let $\beta$ be an element of $\mathcal{F}$ that generates a cycle of length $h$. Now it follows from Theorem 1.10 that $\beta$ generates a subfield $\mathbb{F}_p(\beta) \subseteq \mathcal{F}$ of order $p^h$. Applying Theorem 1.5 to $\mathbb{F}_p(\beta)$ we derive that $\mathbb{F}_p(\beta)$ (and therefore $\mathcal{F}$) contains an element $\alpha$ of order $p^h - 1$. But from the proof of Theorem 1.5 it follows that all the elements of $\mathcal{F}$ have an order that divides $p^k - 1$. In particular we must have $p^h - 1 \;\preceq\; p^k - 1$ and Lemmma 1.3 yields that $h \;\preceq\; k$ completing our proof.

## Proposition 1.10

*Let $\mathcal{F}$ be a field of order $q$ and let $I_d(\mathcal{F})$ denote the number of monic polynomials of degree $d$ in $\mathcal{F}[x]$ which are irreducible in $\mathcal{F}[x]$. This given we have*

$$q^n \;=\; \sum_{d\,\preceq\, n} dI_d(\mathcal{F}) \qquad (\textit{for all } n\geq 1) \tag{1.69}$$

*an therefore from Theorem 1.1 it follows that*

$$I_m(\mathcal{F}) \;=\; \frac{1}{m}\sum_{n\,\preceq\, m} q^n\mu(\tfrac{m}{n}) \tag{1.70}$$

## Proof

Let $\mathcal{M}[\mathcal{F})$ denote the collection of all monic polynomials in $\mathcal{F}[x]$ and let $\mathcal{IM}(\mathcal{F})$ be the subcollection of irreducible ones. Note that if

$$\mathcal{IM}(\mathcal{F}) \;=\; \big\{\phi_1,\phi_2,\phi_3,\ldots,\phi_r,\ldots\big\}$$

then, by Theorem 1.1, every $P\in\mathcal{M}(\mathcal{F})$ may be uniquely expressed in the form

$$P \;=\; \phi_{i_1}^{\alpha_1}\phi_{i_2}^{\alpha_2}\cdots\phi_{i_k}^{\alpha_k} \qquad (\text{for some } 1\leq i_1<i_2<\cdots<i_k).$$

In other words every $P\in\mathcal{M}(\mathcal{F})$ may be viewed as a monomial in the infinite set of variables $\phi_1,\phi_2,\phi_3,\ldots,\phi_r,\ldots$. In this vein, the unique factorization result may simply be translated into the formal power series identity

$$\sum_{P\in\mathcal{M}(\mathcal{F})} P \;=\; \prod_{i\geq 1}(1+\phi_i+\phi_i^2+\cdots) \;=\; \prod_{i\geq 1}\frac{1}{1-\phi_i}. \tag{1.71}$$

Now replacing each polynomial in both sides of 1.71 by the variable $t$ raised to the degree of the polynomial we obtain the degree-generating function identity :

$$\sum_{P\in\mathcal{M}(\mathcal{F})} t^{degree(P)} \;=\; =\; \prod_{i\geq 1}\frac{1}{1-t^{degree(\phi_i)}}. \tag{1.72}$$

Since the total the number of polynomials

$$P(x) \;=\; c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}+x^n \qquad (\text{with } c_i\in\mathcal{F} \text{ for all } 0\leq i<n)$$

is clearly $q^n$, by grouping together terms of equal degree in 1.72, gives the beautiful formal series identity

$$\frac{1}{1-qt} \;=\; \sum_{n\geq 0} q^nt^n \;=\; \prod_{d\geq 1}\Big(\frac{1}{1-t^d}\Big)^{I_d(\mathcal{F})}. \tag{1.73}$$

Using the basic identity

$$\tfrac{1}{1-u} \;=\; \exp\big(\textstyle\sum_{n\geq 1}\frac{u^n}{n}\big) \tag{1.74}$$

for $u = qt$ and $u = t^d$ in 1.73 and and equating logarithms of both sides gives

$$\begin{aligned}\sum_{n\geq 1}\frac{q^n t^n}{n} &= \sum_{d\geq 1} I_d(\mathcal{F})\sum_{m\geq 1}\frac{t^{dm}}{m}\\ &= \sum_{d\geq 1} dI_d(\mathcal{F})\sum_{m\geq 1}\frac{t^{dm}}{dm}\\ &= \sum_{n\geq 1} dI_d(\mathcal{F})\sum_{n\geq 1}\frac{t^n}{n}\chi(d \preceq n)\\ &= \sum_{n\geq 1}\frac{t^n}{n}\sum_{d \preceq n} dI_d(\mathcal{F})\end{aligned}$$

and 1.70 is obtained by equating coefficients of $t^n$ on both sides of this identity.

## Theorem 1.13

*For any integer $k \geq 1$ the polynomial $x^{p^k} - x$ factors into the product of all irreducible monic polynomials in $\mathbb{F}_p[x]$ whose degree divides $k$. That is, if $\mathcal{IM}(\mathbb{F}_p)$ denotes the collection of monic polynomials in $\mathbb{F}_p[x]$ that are irreducible in $\mathbb{F}_p[x]$ we have*

$$x^{p^k} - x = \prod_{\substack{\phi\in\mathcal{IM}(\mathbb{F}_p)\\ degree(\phi) \preceq k.}} \phi(x) \tag{1.75}$$

*In particular it follows from 1.75 that in any finite field $\mathcal{F}$ of order $p^k$ every irreducible polynomial $\phi(x) \in \mathbb{F}_p[x]$ whose degree divides $k$ splits into a product of linear factors.*

## Proof

Let $\mathcal{F}$ be a finite field of order $p^k$ and let $\Delta \subseteq \mathcal{F}$ be a set of representatives of the Frobenius cycles of $\mathcal{F}$. This given, we have the factorization

$$x^{p^k} - x = \prod_{\beta\in\Delta}\phi_\beta(x) \tag{1.76}$$

where $\phi_\beta(x)$ is the polynomial defined by 1.59. Indeed this identity is an immediate consequence of Theorem 1.9 since it simply expresses the fact that $\mathcal{F}$ breaks up into a union of disjoint Frobenis cycles. It develops that 1.75 and 1.76 are one and the same factorization. To see this let $\mathcal{IM}_h(\mathbb{F}_p)$ denote the collection of elements of $\mathcal{IM}(\mathbb{F}_p)$ that are of degree $h$ and likewise let $\mathcal{JM}_h$ denote the collection factors $\phi_\beta(x)$ in 1.75 that are of degree $h$. Since we have shown that each $\phi_\beta(x)$ is monic and irreducible in $\mathbb{F}_p[x]$ and of degree a divisor of $k$ we necessarily have the containment

$$\mathcal{JM}_h \subseteq \mathcal{IM}_h(\mathbb{F}_p) \qquad \text{for all } h \preceq k \tag{1.77}$$

Thus to prove that the factorization in 1.75 and 1.76 are identical we need only show that we have equality in 1.76 for all $h \preceq k$. Now note that Proposition 1.10, for $\mathcal{F} = \mathbb{F}_p$ and $q = p$ yields the identity

$$\sum_{h \preceq k} hI_h(\mathcal{F}) = p^k. \tag{1.78}$$

where $I_h(\mathcal{F})$ is none other than the cardinality of $\mathcal{IM}_h(\mathbb{F}_p)$. On the other hand if $J_h(\mathcal{F})$ denotes the cardinality of $\mathcal{JM}_h$ it follows from 1.77 that

$$J_h(\mathcal{F}) \le I_h(\mathcal{F}). \tag{1.79}$$

Now if any of these inequalities were to be strict we would have

$$\sum_{h \preceq k} hI_h(\mathcal{F}) < p^k.$$

But that would immediately lead to a contradiction since comparing degrees of both sides of 1.75 yields the equality

$$\sum_{h \preceq k} hI_h(\mathcal{F}) = p^k.$$

Thus equality must hold true for all $h \preceq k$ in both 1.79 and 1.77 as desired. This proves that 1.75 and 1.76 are identical factorizations, in particular it follows that each monic irreducible polynomial in $\mathbb{F}_p[x]$ whose degree is a divisor of $k$ splits into a product of linear factors whose roots are the elements of a Frobenius cycle of $\mathcal{F}$. This completes our proof.

The factorization in 1.76 has a useful by-product which is worth noting

## Proposition 1.11

*Let $\mathcal{F}$ be a field of order $p^k$ and let $\Delta$ be a set of representatives of the Forbenius cycles of $\mathcal{F}$. This given we have the factorization*

$$Q_d(x) \;=\; \prod_{\substack{\beta\in\Delta \\ ord(\beta)=d}} \phi_\beta(x) \qquad (\textit{for all } d \preceq p^k-1) \tag{1.80}$$

*where again $\phi_\beta(x)$ is given by 1.59.*

## Proof

The identity in 1.44, which holds true in all finite fields of order $q$, specialized to a field $\mathcal{F}$ of order $p^k$ gives the factorization

$$x^{p^k-1}-1 \;=\; \prod_{d \preceq p^k-1} Q_d(x)\,. \tag{1.81}$$

On the other hand 1.76 gives

$$x^{p^k-1}-1 \;=\; \prod_{\substack{\beta\in\Delta \\ \beta\neq 0}} \phi_\beta(x) \;=\; \prod_{d \preceq p^k-1} \;\prod_{\substack{\beta\in\Delta \\ ord(\beta)=d}} \phi_\beta(x) \tag{1.82}$$

Since the roots of $Q_d(x)$ are all the elements of order $d$ in $\mathcal{F}$, from 1.81 and 1.82 it follows that each $\beta \in \Delta$ that is of order $d$ must be a root of $Q_d(x)$. But since, by Proposition 1.7, $p$ cannot be a divisor of $d$ it follows that if $\beta$ is of order $d$ then all powers $\beta^{p^s}$ are also of order $d$. This gives that if $\beta$ is a root of $Q_d(x)$ all the elements of the Frobenius cycle of $\beta$ must also be roots of $Q_d(x)$. Of course the same conclusion would be reached using the irreducibility of $\phi_\beta(x)$. Thus 1.80 is an immediate consequence of 1.81 and 1.82.

We are now in a position to establish one of the fundamental results in the theory of finite fields.

## Theorem 1.14

*Within a field $\mathcal{F}$ of order $p^k$ lies one and only one subfield $\mathcal{F}_h$ of order $p^h$ for any $h \preceq k$ and it simply consists of the roots of the polynomial $x^{p^h} - x$. That is*

$$\mathcal{F}_h \;=\; \big\{\beta \in \mathcal{F} \,:\, \beta^{p^h} = \beta\big\}\,. \tag{1.80}$$

*Moreover, the collection $\{\mathcal{F}_h\}_{h \preceq k}$, under containment, is isomorphic to the partial order of the divisors of $k$. In particular all fields of order $p^k$ are isomorphic.*

## Proof

Let us say that an integer $d$ "*belongs to the exponent* $h$ " and write "$exp(d) = h$" if $h$ is the order of $p$ in the integers mod $d$. It follows from Theorem 1.10 that an element $\beta \in \mathcal{F}$ of order $d$ generates a subfield $\mathbb{F}_p[\beta]$ of order $p^h$ if and only if $exp(d) = h$. We claim that for all $\gamma \in \mathcal{F}$ with $exp\big(ord(\gamma)\big) = h$ we have

$$\mathbb{F}_p[\gamma] \;=\; \mathcal{F}_h. \tag{1.81}$$

To show this let us pick a $d \preceq p^k - 1$ that belongs to the exponent $h$ and any $\gamma \in \mathcal{F}$ of order $d$. Now if $\alpha$ is a primitive root of $\mathbb{F}_p[\gamma]$ then

$$\mathbb{F}_p[\gamma] \;=\; \big\{0, \alpha, \alpha^2, \ldots, \alpha^{p^h-1}\big\}. \tag{1.82}$$

In particular all elements of $\mathbb{F}_p[\gamma]$ are roots of the polynomial

$$x^{p^h} - x.$$

Since this polynomial cannot have more than $p^h$ roots in $\mathcal{F}$ we see that in $\mathcal{F}$ we have

$$\beta^{p^h} - \beta \;=\; 0 \qquad \Longleftrightarrow \qquad \beta \in \mathbb{F}_p[\gamma]. \tag{1.83}$$

This proves 1.81. Note further that since in $\mathbb{F}_p[\gamma]$ we have the factorization

$$x^{p^h-1} - 1 \;=\; \prod_{d' \,\preceq\, p^h-1} Q_{d'}(x)$$

it follows that every element $\beta \in \mathcal{F}$, that is of order $d' \preceq p^h - 1$, must necessarily lie in $\mathbb{F}_p[\gamma]$, thus in $\mathcal{F}_h$. In particular the subfield $\mathbb{F}_p[\beta]$ it generates must entirely lie in $\mathcal{F}_h$. But if $exp(d') = h'$ then $\mathbb{F}_p[\beta] = \mathcal{F}_{h'}$ . This gives

$$\mathcal{F}_{h'} \subseteq \mathcal{F}_h \qquad \Longleftrightarrow \qquad h' \preceq h$$

Note further that in the particular case $h = k$ we have shown that

$$\mathcal{F}_k \;=\; \mathbb{F}_p[\beta] = \mathcal{F} \qquad (\text{for all } \beta \in \mathcal{F} \text{ such that } exp(ord(\beta)) = k). \tag{1.84}$$

Since the field $\mathbb{F}_p[\beta]$ is isomorphic to the quotient field $\mathbb{F}_p[x]/(\phi_\beta(x))$. From 1.75 we derive that if we take any polynomial $f(x) \in \mathbb{F}_p[x]$ of degree $k$ that is irreducible in $\mathbb{F}_p[x]$ then the quotient field $\mathbb{F}_p[x]/(f(x))$ is isomorphic to $\mathcal{F}$. This proves the equality of all fields of order $p^k$ and completes our proof.

Here and after the unique field of order $p^k$ will be denoted $\mathbb{F}_{p^k}$. One of the by-products of this subsection is that no matter how $\mathbb{F}_{p^k}$ is constructed it contains whithin itself all possible ways of constructing it. We shall call the quotient construction $\mathbb{F}_p[x]/(f(x))$ with $f(x) \in \mathbb{F}_p[x]$ irreducible of degree $k$ a "*presentation of* $\mathbb{F}_{p^k}$". But we should keep in mind that although they all yield the same field, some presentations may be more efficient than others in computer experimentations.

## 1.4 A Factorization Algorithm

It follows from the results in the previous subsection that every ireducible polynomial $f(x) \in \mathbb{F}_p[x]$ of degree a divisor of $k$ splits into product of linear factors in $\mathbb{F}_{p^k}$. In this subsection we shall give an algorithm for carrying out such factorizations.

Our basic tool here will be the polynomial

$$S_k(x) \;=\; x + x^p + x^{p^2} + \cdots + x^{p^{k-1}} \tag{1.85}$$

for some prime $p$.

**Proposition 1.12**

1) $S_k(x)$ *maps* $\mathbb{F}_{p^k}$ *onto* $\mathbb{F}_p$
2) $cS_k(x) = S_k(cx)$ *for all* $c \in \mathbb{F}_p$.
3) *for all* $\alpha, \beta \in \mathbb{F}_{p^k}$ *we have* $S_k(\alpha+\beta) = S_k(\alpha) + S_k(\beta)$
4) *If* $\beta \in \mathbb{F}_{p^k}$ *we have* $S_k(\beta x) = 0$ *for all* $x \in \mathbb{F}_{p^k}$ *if and only if* $\beta = 0$

**Proof**

Note that, from Theorem 1.14 we derive that

$$S_k(\beta)^p \;=\; \beta^p + \beta^{p^2} + \cdots + \beta^{p^k} \;=\; S_k(\beta) \qquad (\text{for all } \beta \in \mathbb{F}_{p^k}) \tag{1.86}$$

This proves that $S_k(x)$ maps $\mathbb{F}_{p^k}$ into $\mathbb{F}_p$. Note further that for $c \in \mathbb{F}_p$ we have $c^{p^s} = c$ for all $s \geq 0$ thus

$$S_k(cx) \;=\; cx + c^p x^p + + \cdots + c^{p^{k-1}} x^{p^{k-1}} \;=\; cS_k(x).$$

This proves 2). Recall that in a field of characteristic $p$ we have the identity

$$(\alpha+\beta)^{p^s} \;=\; \alpha^{p^s} + \beta^{p^s} \qquad (\text{for all } s \geq 0)$$

This proves 3).

Next note that if $\beta \neq 0$ in $\mathbb{F}_{p^k}$ then

$$S_k(\beta x) \;=\; x\beta + x^p\beta^p + x^{p^2}\beta^{p^2} + \cdots + x^{p^{k-1}}\beta^{p^{k-1}}$$

is a polynomial of degree $p^{k-1} < p^k$ and cannot identically vanish in $\mathbb{F}_{p^k}$. This proves 4). We are left to show that $S_k(x)$ is onto. Note first that the equation $S_k(x) = 0$ cannot have more than $p^{k-1}$ solutions in $\mathbb{F}_{p^k}$. Since $\mathbb{F}_{p^k}$ has $p^k$ elements we can certainly find $\beta \in \mathbb{F}_{p^k}$ such that

$$S_k(\beta) \neq 0$$

Let then $S_k(\beta) = c_o$. Now 1.86 gives that $c_o \in \mathbb{F}_p$ and from 2) we derive that

$$S_k(\beta/c_o) = 1$$

but then again from 2) it follows that

$$S_k(i\beta/c_o) = i \qquad \text{for all} \quad i = 0, 1, 2, \ldots, p-1$$

This proves that $S_k(x)$ is onto and completes our argument.

## Proposition 1.13

*For any $c \in \mathbb{F}_p$ the equation*

$$S_k(x) \;=\; c \tag{1.86}$$

*has exactly $p^{k-1}$ solutions in $\mathbb{F}_{p^k}$.*

## Proof

Properties 1), 2) and 3) of Proposition 1.12 yield that that $S_k$ is a linear tranformation of $\mathbb{F}_{p^k}$ onto $\mathbb{F}_p$ as vector spaces over $\mathbb{F}_p$. Since $\mathbb{F}_{p^k}$ is a $k$ dimensional space over $\mathbb{F}_p$ and the dimension of the range of $S_k$ is 1 it follows that the dimension of the nullspace of $S_k$ must be $k-1$. Thus the equation

$$S_k(x) = 0$$

has exactly $p^{k-1}$ solutions in $\mathbb{F}_{p^k}$. Now note that for any two elements $\beta_1, \beta_2 \in \mathbb{F}_{p^k}$ we have, by 3) of Proposition 1.12

$$S_k(\beta_2 - \beta_1) + S_k(\beta_1) \;=\; S_k(\beta_2) \tag{1.87}$$

This shows that if $S_k(\beta_1) = c$ for some $c \in \mathbb{F}_p$ then $S_k(\beta_2) = c$ if and only if $S_k(\beta_2 - \beta_1) = 0$. Thus the solution set of 1.86 can be obtained by adding to a particular solution of $S_k(x) = c$ a solution of $S_k(x) = 0$. Since we have seen that $S_k(x) = 0$ has exactly $p^{k-1}$ solutions and $S_k$ is an onto map, it follows that the equation in 1.86 has exactly $p^{k-1}$ solutions for all $c \in \mathbb{F}_p$.

Proposition 1.13 has the following remarkable corollary

## Theorem 1.15

$$x^{p^k} - x \;=\; \prod_{c \in \mathbb{F}_p} (S_k(x) - c) \tag{1.88}$$

## Proof

Note that if

$$S_k(\beta_1) = c_1 \qquad \text{and} \qquad S_k(\beta_2) = c_2$$

then

$$c_1 \neq c_2 \qquad \Longrightarrow \qquad \beta_1 \neq \beta_2$$

Thus the solution sets

$$\big\{\beta \in \mathbb{F}_{p^k} \,:\, S_k(\beta) = c\big\}$$

are disjoint as $c$ varies in $\mathbb{F}_p$. Since each of them has $p^{k-1}$ elements and there are altogether $p$ of them it follows that their union must necessarily be all of $\mathbb{F}_{p^k}$. This proves 1.88.

We are finally in a position to prove the crucial result of this subsection.

## Theorem 1.16

*Let $\alpha$ be a primitive root of $\mathbb{F}_{p^k}$ and $f(x) \in \mathbb{F}_p[x]$ be a monic polynomial with distinct roots in $\mathbb{F}_{p^k}$ then for each $0 \le j \le p^k - 1$ we have the factorization*

$$\alpha^j f(x) \;=\; \prod_{c\in\mathbb{F}_p} gcd\big(f(x), S_k(\alpha^j x) - c\,\big) \tag{1.89}$$

*Moreover for at least one $0 \le j \le p^k - 1$ this factorization is not trivial.*

## Proof

By assumption we have

$$f(x) \;=\; (x-\beta_1)(x-\beta_2)\cdots(x-\beta_h)$$

with $\beta_1, \beta_2, \ldots, \beta_h$ distinct elements of $\mathbb{F}_{p^k}$. Now 1.88 with $x$ replaced by $\alpha^j x$ gives

$$\alpha^j(x^{p^k} - x) \;=\; \prod_{c\in\mathbb{F}_p} (S_k(\alpha^j x) - c) \tag{1.89}$$

Thus every $\beta_j$ must be a root of the polynomial on the right. This gives the factorization in 1.89. Now this factorization is trivial, for a given $j$, only if for some $c_o \in \mathbb{F}_p$ we have that $f(x)$ divides $S_k(\alpha^j x) - c_o$. This means that

$$S_k(\alpha^j \beta_r) = c_0 \qquad (\text{for all } r = 1, 2, \ldots, h)$$

But then from the identity in 1.87 it follows that

$$S_k\big(\alpha^j(\beta_r - \beta_s)\big) \;=\; S_k(\alpha^j\beta_r) - S_k(\alpha^j\beta_s) \;=\; 0 \qquad \text{for all } 1 \le r < s \le h$$

Now if this were to hold for all $j = 1, 2, \ldots, p^k - 1$ then from 4) of Proposition 1.12 it would follow that

$$\beta_r = \beta_s$$

contradicting the asssumption that $\beta_1, \beta_2, \ldots, \beta_h$ are distict. This contradiction proves our assertion and completes our proof.

**Note:** Using Theorem 1.16 it is easy to put together an algorithm that completely factorizes every polynomial in $\mathbb{F}_p[x]$ with roots in $\mathbb{F}_{p^k}$.