Cryptography and Security of Digital Devices

Notes on abstract algebra and modular arithmetic

Finite Fields

Gerardo Pelosi

Exam Code 090959 – A.Y. 2013-2014, Semester 2
Politecnico di Milano

1 Field Extensions

Let $\mathbb{F}$ be a field. A subset $\mathbb{K}$ of $\mathbb{F}$ that is itself a field under the operations of $\mathbb{F}$ will be called a *subfield* of $\mathbb{F}$. In this context, $\mathbb{F}$ is called an *extension field* of $\mathbb{K}$. If $\mathbb{K} \neq \mathbb{F}$, we say $\mathbb{K}$ is a *proper* subfield of $\mathbb{F}$.

From these definitions it is possible to infer that $\mathbb{Z}_p{=}\mathbb{F}_p$ has no proper subfield.

Indeed, assuming $\mathbb{K}$ is a subfield of a finite field $\mathbb{Z}_p{=}\mathbb{F}_p$, p prime, then $\mathbb{K}$ must contain 0, and 1, and so all other elements of $\mathbb{F}_p$ by the closure of $\mathbb{K}$ under addition. Therefore, it follows that $\mathbb{Z}_p{=}\mathbb{F}_p$ contains no proper subfield.

Definition 1.1 (Prime Field)**.** *A field containing no proper subfield is called* prime *field.*

Theorem 1.1 (Isomorphism of finite fields)**.** *The prime subfield of a field $\mathbb{F}$ is isomorphic to either $\mathbb{F}_p$, with p prime, or to $\mathbb{Q}$ depending on whether the cardinality of the field is finite or infinite.*

Definition 1.2 (Extension field)**.** *Let $\mathbb{K}$ be a subfield of $\mathbb{F}$, and $\mathbf{M}$ a generic subset of $\mathbb{F}$. $L = \mathbb{K}(\mathbf{M})$ denotes the field defined as the intersection of all subfields of $\mathbb{F}$ containing both $\mathbb{K}$ and $\mathbf{M}$.*
L usually denominated "extension field" of $\mathbb{K}$. The support set of L is obtained through "adjoining" the elements of $\mathbf{M}$ to $\mathbb{K}$. If $\mathbf{M}$ includes a single element $M{=}\{\alpha\}{\in}\mathbb{F}$ then $L{=}\mathbb{K}(\alpha)$ is called simple extension of $\mathbb{K}$, and α is the defining element of L over $\mathbb{K}$.

Given a Field $\mathbb{K}$, our objective will be to state the conditions to represent the set of objects composed by the elements of $\mathbb{K}$ plus a further object (symbolically denoted as $\alpha{\notin}\mathbb{K}$) and as a Field. Note that, also all possible compositions of α and the elements of $(\mathbb{K}, +, \cdot)$ will be included as elements of the Field. We will denote it as $\mathbb{F}{=}\mathbb{K}(\alpha)$, and call it "extension field" of $\mathbb{K}$.

Definition 1.3 (Minimal Polynomial)**.** *Let $\mathbb{K}$ be a proper subfield of $\mathbb{F}$, and let α be a generic element of $\mathbb{F}$, (i.e., $\alpha{\in}\mathbb{F}$). If $g(x){\in}\mathbb{K}[x]$ is the monic polynomial with the least degree such that $g(\alpha){=}0$, then α is called* algebraic element over $\mathbb{K}$*, whereas $g(x)$ is called* minimal polynomial *of α over $\mathbb{K}$.*

Note that if $\alpha{\in}\mathbb{K}$, then its minimal polynomial in $\mathbb{K}[x]$ is the linear one:
$g(x) = x{-}\alpha{\in}\mathbb{K}[x]$. Therefore, the interesting things will happen when $\alpha{\in}\mathbb{F}\backslash\mathbb{K}$:

Theorem 1.2. *Let $\alpha{\in}\mathbb{F}$ be an algebraic element over $\mathbb{K}$: its minimal polynomial $g(x){\in}\mathbb{K}[x]$ has the following properties:*

1. *$g(x)$ is irreducible in $\mathbb{K}[x]$.*
2. *For $f(x){\in}\mathbb{K}[x]$ we have $f(\alpha){=}0$, if and only if $g(x)$ divides $f(x)$.*

1.1 Simple algebraic extensions

The elements of a simple algebraic extension field $\mathbb{K}(\alpha)$ with minimal polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{K}[x]$, (i.e., the smallest field including α and $\mathbb{K}$) are polynomial expressions in α. Any element in $\mathbb{K}(\alpha)$ may be uniquely represented in the form $b_{n-1}\alpha^{n-1} + \ldots + b_1\alpha + b_0$ with $b_i \in \mathbb{K}$, for $0 \leq i \leq n-1$. Note that any power of α greater than or equal to α^n can be reduced using the equality given by the minimal polynomial $\alpha^n = -(a_{n-1}\alpha^{n-1} + \ldots + \alpha)$.

Theorem 1.3. *Let $L = \mathbb{K}(\alpha)$ be a simple algebraic extension field, with $f(x) \in \mathbb{K}[x]$ being the minimal polynomial of α over $\mathbb{K}$. Then, L is isomorphic to the field $\mathbb{K}[x]/\langle f(x)\rangle$.*

Example 1.1. *As an example of the formal process of root adjunction consider the field $\mathbb{K} = \mathbb{Z}_3$ and the polynomial $f(x) = [1]x^2 + [1]x + [2]$ irreducible in $\mathbb{Z}_3$. The field $L = \mathbb{Z}_3[x]/\langle f(x)\rangle$ includes as elements*

$$L = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$$

(as usual, for the sake of simplicity, each equivalence class in $\mathbb{Z}_3$ is identified with a representative element (i.e., zero or the smallest positive one), while each polynomial should be viewed as the representative element of its coset of $\langle f(x)\rangle$ in $\mathbb{Z}_3[x]$)

Now let α be a root of $f(x)$ in $L = \mathbb{Z}_3[x]/\langle f(x)\rangle$, say $\alpha = x + \langle f(x)\rangle$ therefore, L can be viewed as a simple extension of $\mathbb{K} = \mathbb{Z}_3$ with α:

$$L = \mathbb{Z}_3(\alpha) = \{\alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2, 0, 1, 2\}$$

Another root of $f(x) \in L$ is $2\alpha + 2$, since

$$f(2\alpha+2) = (2\alpha+2)^2 + (2\alpha+2) + 2 = \alpha^2 + \alpha + 2 = 0 \text{ in } L$$

The set of all possible polynomials generated by $2\alpha + 2$ is

$$L = \mathbb{Z}_3(2\alpha+2) = \{2\alpha+2, 2\alpha, 2\alpha+1, \alpha+1, \alpha, \alpha+2, 1, 0, 2\}$$

Therefore, we may adjoin either the root $\alpha \in L$ or the root $2\alpha + 2 \in L$ of $f(x) \in \mathbb{K}[x]$ to the field $\mathbb{K} = \mathbb{Z}_3$ obtaining the same field.

The situation in the above example is covered by the following:

Theorem 1.4. *Let α, β be two roots of the polynomial $f(x) \in \mathbb{K}[x]$ that is irreducible over $\mathbb{K}[x]$. The extension fields $\mathbb{K}(\alpha), \mathbb{K}(\beta)$ are isomorphic. The map between the two simply maps α to β and keeps the elements of $\mathbb{K}$ fixed.*

A particular extension of a field, which is really useful, is the one where all roots of a given polynomial belong.

Definition 1.4 (Splitting Field)**.** *Let $f(x) \in \mathbb{K}[x]$ be a polynomial with degree greater than zero, and $\mathbb{F}$ an extension field of $\mathbb{K}$. Then $f(x)$ is said to* **split** *in $\mathbb{F}$, if*

1. *$f(x)$ can be written as the product of linear factors with roots in $\mathbb{F}$: $f(x) = a\prod_i (x - \alpha_i)$, $\alpha_i \in \mathbb{F}$, $a \in \mathbb{K}$*
2. *$\mathbb{F}$ is an algebraic extension of $\beta_i : f(\beta_i) = 0, \forall i$: $\mathbb{F} = \mathbb{K}(\beta_1, \ldots, \beta_i, \ldots)$. In this case, $\mathbb{F}$ is said to be a "splitting field" of $f(x)$ over $\mathbb{K}$.*

It is possible to prove the following:

Theorem 1.5. *Let $\mathbb{K}$ be a field and $g(x) \in \mathbb{K}[x]$ be a polynomial with positive degree $n > 0$, then there exists a unique splitting field $\mathbb{F}$ of $g(x)$ over $\mathbb{K}$ (up to an isomorphism mapping the roots of $f(x)$ among them and keeping the elements of $\mathbb{K}$ fixed).*

Proof. To build a "splitting field" we consider the unique factorization of $g(x)$ in irreducible factors $g(x) = a\prod_i^r g_i(x)$, $r < n$, $a \in \mathbb{K}$. Let $g_i(x)$ be the first factor with degree greater than 1, then we build $\mathbb{K}_1 = \mathbb{K}[x]/ < g_i(x) >$. As previously observed, $g_i(x)$ has an obvious root when considered with coefficients in $\mathbb{K}_1$ say θ, and $\mathbb{K}_1 = \mathbb{K}(\theta)$.

Now consider a new factorization of $g(x)$ in $\mathbb{K}_1$ and repeat the above procedure. As the sum of the degrees in the factorization of $g(x)$ is less than n, and for each step at least one factor decreases its degree, it is possible to infer that in a finite number of steps we build a field, $\mathbb{F}$, over which $g(x)$ can be written as the product of linear factors. This field $\mathbb{F}$ is splitting filed of $\mathbb{K}$.
The uniqueness of such a field is proven through a generalization of Theorem 1.5. □

2 Characterization of Finite Fields

Given a finite field $\mathbb{K}$ with order $q = |\mathbb{K}|$, we have seen that its simple extension $\mathbb{F}$ can be built as $\mathbb{K}[x]/\langle f(x)\rangle \equiv \mathbb{K}(\alpha)$ with $f(x) \in \mathbb{K}[x]$ irreducible, $n = deg(f(x))>1$ and $f(\alpha) = 0$, $\alpha \in \mathbb{F}\setminus\mathbb{K}$. The order of the field $\mathbb{F}$ is $|\mathbb{F}| = |\mathbb{K}|^n$.

1. $\mathbb{F}_p = \mathbb{Z}_p = \mathbb{Z}/\langle p\rangle = \mathbb{Z}/p\mathbb{Z}$ (with p prime) is a "prime subfield"
2. In every finite field (prime or extended/composite) if $\mathbb{F}_p$ is its prime subfield, then for any element $a\in\mathbb{F}$ is it true that:
   $pa = \underbrace{a + a + \ldots + a}_{p \text{ times}} = 0$
   The value p is called **characteristic of the field** $\mathbb{F}$.
3. For all $a \in \mathbb{K}$, with $q = |\mathbb{K}|$ it is always true that $a^q = a$.
   This is due to the fact that, the multiplicative group of the field $(\mathbb{K}^*, \cdot)$ has order $q - 1$ and thus, $a \in \mathbb{K}\setminus\{0\}, a^{q-1} = 1$.
4. Let p be the characteristic of the finite field $\mathbb{K}$, then $\forall\, a, b \in \mathbb{K}$, $m \geq 1$ we have:

$$(a\pm b)^{p^m} = \sum_{i=0}^{p^m} \binom{p^m}{i} a^i(\pm b)^{p^m-i} = \sum_{i=0}^{p^m} \frac{p^m(p^m-1)\cdots(p^m-i+1)}{i(i-1)\cdots 2\cdot 1} a^i(\pm b)^{p^m-i} =$$

$$= \binom{p^m}{p^m} a^{p^m}(\pm b)^{p^m-p^m} + \binom{p^m}{0} a^0(\pm b)^{p^m-0} = a^{p^m} \pm b^{p^m}$$

Proposition 2.1. *Every finite field $\mathbb{K}$ has order p^n where p is the characteristic of $\mathbb{K}$ and $n \geq 1$.*

Theorem 2.1 (Existence and Uniqueness of a Finite Field)**.** *For every prime p and every positive integer n, there exists a finite field $\mathbb{F}_q$ with $q = p^n$ elements. In particular, every finite field $\mathbb{F}_q$ with $q = p^n$ elements is isomorphic to the splitting field of $x^q - x \in \mathbb{Z}_p[x]$, that is $x^q - x = \prod_{a\in\mathbb{F}_q}(x - a)$.*

Theorem 2.2. *Let $\mathbb{F}_q$ be the finite field with $q = p^n$ elements. Then every subfield of $\mathbb{F}_q$ has order p^m, where m is a positive divisor of n. Conversely, if m is a positive divisor of n, then there exists exactly one subfield of $\mathbb{F}_q$ with p^m elements.*

Example 2.1. *Let $\mathbb{F}_{2^{12}}$ be a field, then its subfields are:*
$\mathbb{F}_2 < \mathbb{F}_{2^2} < \mathbb{F}_{2^4} < \mathbb{F}_{2^{12}}$
$\mathbb{F}_2 < \mathbb{F}_{2^3} < \mathbb{F}_{2^6} < \mathbb{F}_{2^{12}}$

Theorem 2.3. *For every finite field $\mathbb{F}_q$, the multiplicative group $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$ is cyclic with order $q-1$.*

Definition 2.1 (Primitive Element)**.** *A generator of the cyclic group $\mathbb{F}_q^*$ is called* ***primitive*** *element of $\mathbb{F}_q$.*

We note that *if $\mathbb{H}$ and $\mathbb{K}$ are two finite fields and $\mathbb{H}$ is a subfield of $\mathbb{K}$ ($\mathbb{H} < \mathbb{K}$) then, $\mathbb{K}$ is a simple algebraic extension of $\mathbb{H}$ defined by any primitive element ξ of $\mathbb{K}$.* Indeed, ξ is algebraic over $\mathbb{H}$ because ξ is a root of $x^{|\mathbb{K}|-1} - 1 \in \mathbb{H}[x]$, moreover $\mathbb{H}(\xi) \subseteq \mathbb{K}$. Now, note that 0 and all the powers of ξ are included in $\mathbb{H}(\xi)$ thus, $\mathbb{K} \subseteq \mathbb{H}(\xi)$ (as $\mathbb{K}^*$ is cyclic, with generator ξ, $(\mathbb{K}^*, \cdot) = (\langle \xi \rangle, \cdot)$). We infer that $\mathbb{K} = \mathbb{H}(\xi)$.
From this, we further infer that there exists a minimal polynomial for ξ over $\mathbb{H}$, and that this polynomial is irreducible over $\mathbb{H}$.
In particular, the finite field $\mathbb{F}_{p^n}$ is a simple extension of $\mathbb{Z}_p$, defined by a primitive element of $\mathbb{F}_{p^n}$. This element must have a minimal polynomial with degree n over $\mathbb{Z}_p$ thus, there always exists an irreducible polynomial with degree n in $\mathbb{Z}_p[x]$.

Corollary 2.1. *If g is a primitive element of a finite field $\mathbb{F}_q$, then every primitive element is in $\{g^h$ s.t. $gcd(q-1, h) = 1,\ h = 1, 2, \ldots, q-2\}$. In particular, the number of primitive elements is $\varphi(q-1)$.*

Corollary 2.2. *Let $\mathbb{F}_p$, with p prime, be a finite field and g a primitive element, then, for all r, such that $r \mid p-1$, it holds that $g^{\frac{p-1}{r}} \neq 1 \bmod p$*

Example 2.2. *We employ the previous corollary to find a primitive element of $\mathbb{F}_{11}$:*
$g \overset{Random}{\leftarrow} \{1, 2, \ldots, 10\}$.
F.i., $g = 2$, $p - 1 = 10 = 2 \cdot 5$

$$g^{\frac{p-1}{2}} = g^5 = 10 \neq 1$$
$$g^{\frac{p-1}{5}} = g^2 = 4 \neq 1$$

therefore, $g = 2$ is a primitive element!

Definition 2.2 (Primitive Polynomial)**.** *Let $g(x) \in \mathbb{F}_p[x]$ be an irreducible monic polynomial with degree $n = deg(g(x))$. If $g(x)$ is the minimal polynomial of a primitive element $\alpha \in \mathbb{F}_{p^n}$ then $g(x)$ is called a* ***primitive polynomial****.*

Note that the set of primitive polynomials with coefficients in a finite field is included in the set of irreducible ones. The inverse is not always true!

Proposition 2.2. *Let* $g(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{F}_p[x]$ *be a primitive polynomial of* $\mathbb{F}_{p^n} \cong \mathbb{F}_p(\alpha)$, $g(\alpha) = 0$, $\alpha \in \mathbb{F}_{p^n} \backslash \mathbb{F}_p$, *then*

$$0 = g(\alpha) = g(\alpha)^{p^j}, \quad \forall\, j \in \{0, 1, 2, \ldots, n-1\}$$

$$0 = g(\alpha)^{p^j} = (\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0)^{p^j} =$$

$$= ((\alpha^{p^j})^n + a_{n-1}^{p^j}(\alpha^{p^j})^{n-1} + \ldots + a_1^{p^j}(\alpha)^{p^j} + a_0^{p^j}) =$$

$$= ((\alpha^{p^j})^n + a_{n-1}(\alpha^{p^j})^{n-1} + \ldots + a_1(\alpha^{p^j}) + a_0) = g(\alpha^{p^j})$$

Therefore, every primitive polynomial with degree n *has* n *roots. These roots (called* ***conjugate elements****) are the primitive elements of the field* $\mathbb{F}_{p^n}$. *In fact:*

$$|\alpha| = p^n - 1; |\alpha^{p^j}| = \frac{p^n - 1}{gcd(p^n - 1, p^j)} = p^n - 1, \ \forall\, j \in \{1, 2, \ldots, n-1\}$$

2.1 Irreducible and Primitive Polynomials

Theorem 2.4. *The polynomial* $x^{p^n} - x \in \mathbb{F}_p[x]$ *has a unique factorization (up to a change in the order of the factors) composed by the product of* ***all the irreducible polynomials*** *over* $\mathbb{F}_p$, *having degree* d, *where* d *divides* n.

Corollary 2.3. *Let* $N_d(p)$ *be the number of irreducible monic polynomials with coefficients in* $\mathbb{F}_p$ *and degree equal to* d:

$$N_d(p) = |\{g(x) \in \mathbb{F}_p[x] \ s.t\ g(x) \ \textit{is irreducible, monic and degree} \ = d\}|$$

The sum of all the degrees of the factors of $x^{p^n} - x$, *counted with their multiplicity* $N_d(p)$ *is* p^n :

$$deg(x^{p^n} - x) = p^n = \sum_{d|n} N_d(p) \cdot d$$

If $n = 1$ then the number of irreducible polynomials in $\mathbb{F}_p[x]$ with degree $d = 1$ is $N_1(p) = p$, trivially. If n is a prime number (thus its possible factors are only $d = 1$ and $d = n$), then the number of irreducible polynomials in $\mathbb{F}_p[x]$ with degree $d = n$ is derived through the following relations:

$$N_d(p): \ p^d = N_1(p) \cdot 1 + N_d(p) \cdot d \Rightarrow d = \frac{p^d - p}{d}$$

If n is a composite integer, we need to consider its factorization as the product of prime numbers, then we can compute by induction $N_n(p)$ starting with $N_d(p)$ where d is the smallest prime factor. For instance, if we want to find the number of irreducible polynomials in $\mathbb{F}_5[x]$ with degree $n = 6$, we consider $n = 6 = 1 \cdot 2 \cdot 3$,

- 1 divides 6 and $x^{p^1} - x$ divides $x^{p^6} - x$, therefore: $N_1(p) = p = 5$
- 2 divides 6 and $x^{p^2} - x$ divides $x^{p^6} - x$, therefore: $N_2(p) = \frac{p^2 - p}{2} = 10$
- 3 divides 6 and $x^{p^3} - x$ divides $x^{p^6} - x$, therefore: $N_3(p) = \frac{p^3 - p}{3} = 40$

$N_6(p): \ p^6 = 1 \cdot N_1(p) + 2 \cdot N_2(p) + 3 \cdot N_3(p) + 6 \cdot N_6(p) \Rightarrow N_6(p) = 2595$

Lemma 2.1. *Given a finite field $\mathbb{F}_{p^n}$, let d be a divisor of n and*

$$M_d(p) = |\{g(x) \in \mathbb{F}_p[x] \text{ s.t. } g(x) \text{ is primitive }, deg(g(x)) = d\}|$$

be the number of primitive polynomials of degree d. Referring to Theorem 2.4, and remembering that the roots of a primitive polynomial with degree d are a subset of the $\varphi(p^n - 1)$ primitive elements of $\mathbb{F}_{p^n}$, we obtain that:

$$\varphi(p^n - 1) = d \cdot M_d(p)$$

then

$$M_d(p) = \frac{\varphi(p^n - 1)}{d}$$

2.2 Irreducibility Tests

We have previously reported that every non-constant polynomial $f(x) \in \mathbb{K}[x]$ where $\mathbb{K}$ is a field, can be factored as the product of irreducible polynomials:

$$f(x) = \prod_{i=1}^{s} f_i(x)^{e_i}$$

There are two different questions:

1. How do we establish whether $f(x)$ is irreducible or not?
2. How do we find the factorization of a generic polynomial?

In this section we will give explicit criteria to answer to such questions when dealing with finite fields and monic polynomials.

Theorem 2.5 (Irreducibility Criterion)**.** *Let $f(x) \in F_p[x]$ be a monic polynomial with degree m. Then, $f(x)$ is irreducible in $F_p[x]$ if and only if the value of*

$$gcd(f(x), x^{p^h} - x)$$

is a constant (i.e., a zero degree polynomial) for all the values of $h \leq \lfloor \frac{m}{2} \rfloor$

Example 2.3. *Test the irreducibility of $f(x) = x^5 + 2x^4 + 3x^2 + 2x + 4 \in \mathbb{F}_5[x]$.*

Theorem 2.5 suggest to try $h = 1$, $h = 2$.
The case of $h = 1$ is equivalent to verify whether $f(x)$ has a root in $\mathbb{F}_5$:

$f(0) = 4 \neq 0$
$f(\pm 1) = \pm 1 + 2 + 3 \pm 2 + 4 \neq 0$
$f(\pm 2) = \pm 2 + 2 + 3(4) \pm 4 + 4 \neq 0$

$f(x)$ has no roots in $\mathbb{F}_5$.
The case with $h = 2$ implies the following computation:

$$gcd\left(f(x), x^{5^2} - x\right) = \ldots = x^2 + x + 1 \neq \text{ constant}$$

we can conclude that $f(x)$ is reducible!

We thus note that the polynomial ring $\mathbf{R} = \mathbb{F}_p[x]/\langle f(x)\rangle$ is a finite field only when $f(x) \in \mathbb{F}_p[x]$ is irreducible. In addition, if $\mathbf{R}$ is a finite field with $q = p^n$ elements, $n = deg(f(x))$, then $a^q = a,\ \forall\, a \in \mathbf{R}$

Corollary 2.4 (Reducibility Criterion)**.** *Let $f(x) \in \mathbb{F}_p[x]$ be a polynomial with degree $n = deg(f(x))$. $f(x)$ is reducible if there exists $a \in \mathbb{F}_p[x]/\langle f(x)\rangle$ such that $a^{p^n} \ncong a$*

Example 2.4. *Establish whether $f(x) = x^4 + x^2 + 1 \in \mathbb{F}_2[x]$ is reducible or not.*

Assuming

$$R = \mathbb{F}_2[x]/\langle f(x)\rangle \cong \mathbb{F}(\alpha) = \{\theta_0 + \theta_1\alpha + \theta_2\alpha^2 + \theta_3\alpha^3 \mid \theta_i \in \mathbb{F}_2, f(\alpha) = 0\}$$

If R was a field, it would have $q = 2^4$ elements (i.e. $\forall\, a \in R$ it must be true that $a^q = a$ with $\alpha^4 = \alpha^2 + 1$).
Nevertheless, considering the element α:

$$\alpha^q = \alpha^{16} = (\alpha^4)^4 = (\alpha^2{+}1)^4 = \alpha^8{+}1 = (\alpha^4)^2{+}1 = (\alpha^2{+}1)^2{+}1 = \alpha^4 = \alpha^2{+}1 \neq \alpha$$

Therefore, we conclude that R is not a field and $f(x)$ is reducible!

3 Exercises on Fields $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$

3.1 Exercise 1

Consider the following finite field $\mathbb{F}_7 \cong \mathbb{Z}/7\mathbb{Z}$.

(1) Write down the addition and multiplication tables.

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

·	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

(2) Find the number of primitive elements.

If $n = |\mathbb{F}_7^*|$ is the order of the multiplicative group, the number of generators (i.e., primitive elements of the field) is: $\varphi(n) = \varphi(6) = 2$.

(3) Find the generators of the multiplicative group.

We start from checking the smallest elements: if $g = 2$ is a generator then its order must be equal to 6 and not one of the proper divisors of 6, i.e., either 2 or 3: $2^1 = 2,\ 2^2 = 4,\ 2^3 = 8 = 1$, therefore $g = 2$ cannot be a generator, as its order is equal to 3.
Now we try with $g = 3$: $3^1 = 3,\ 3^2 = 2\ mod\ 7,\ 3^3 = 6\ mod\ 7 \neq 1$. In this group

there are only elements of order 1, 2, 3, 6, so we can conclude that $g_0 = 3$ is a generator of $\mathbb{F}_7$.
The other generator is: $g_1 = g_0^5 = 3^5 = 5 \, mod \, 7$.

(4) Find the multiplicative inverse of the following elements:

$$x = 4, \qquad y = 3$$

Employing the group law we have:

$$p = 7, \; x = 4, x^{-1} \, mod \, 7 \equiv_7 4^5 \equiv_7 (4^2 \cdot 4^2 \cdot 4) \equiv_7 2^2 \cdot 4 \equiv_7 \mathbf{2}$$
$$p = 7, \; y = 3, y^{-1} \, mod \, 7 \equiv_7 3^5 \equiv_7 (3^2 \cdot 3^2 \cdot 3) \equiv_7 2^2 \cdot 3 \equiv_7 \mathbf{5}$$

Employing the Euclidean Algorithm we have:

$$p = 7, \; x = 4 \Rightarrow \; 1 = \gcd(7, 4) = 7\xi + 4\eta$$

$$\begin{cases} \underline{u} \leftarrow (7, 1, 0); \\ \underline{v} \leftarrow (4, 0, 1); \end{cases}$$
$$\begin{cases} q = \lfloor \frac{7}{4} \rfloor = 1, \; \underline{w} \leftarrow (7 - 4, 1 - 0, 0 - 1) = (3, 1, -1); \\ \underline{u} \leftarrow (4, 0, 1); \\ \underline{v} \leftarrow (3, 1, -1); \end{cases}$$
$$\begin{cases} q = \lfloor \frac{4}{3} \rfloor = 1, \; \underline{w} \leftarrow (4 - 3 \cdot 1, 0 - 1 \cdot 1, 1 - (-1) \cdot 1) = (1, -1, 2); \\ \underline{u} \leftarrow (3, 1, -1); \\ \underline{v} \leftarrow (1, -1, 2); \end{cases}$$
$$\begin{cases} q = \lfloor \frac{3}{1} \rfloor = 3, \; \underline{w} \leftarrow (3 - 1 \cdot 3, 1 - (-1) \cdot 3, -1 - 2 \cdot 3) = (0, 4, 7); \\ \underline{u} \leftarrow (1, -1, 2); \\ \underline{v} \leftarrow (0, 4, 7); \end{cases}$$

$$d = 1; \; \xi = -1; \; \eta = 2 \Rightarrow x^{-1} = 4^{-1} \, mod \, 7 = \mathbf{2}$$

$$p = 7, \; y = 3 \Rightarrow \; 1 = \gcd(7, 3) = 7\xi + 3\eta$$

$$\begin{cases} \underline{u} \leftarrow (7, 1, 0); \\ \underline{v} \leftarrow (3, 0, 1); \end{cases}$$
$$\begin{cases} q = \lfloor \frac{7}{3} \rfloor = 2, \; \underline{w} \leftarrow (7 - 6, 1 - 0, 0 - 2) = (1, 1, -2); \\ \underline{u} \leftarrow (3, 0, 1); \\ \underline{v} \leftarrow (1, 1, -2); \end{cases}$$
$$\begin{cases} q = \lfloor \frac{3}{1} \rfloor = 3, \; \underline{w} \leftarrow (3 - 1 \cdot 3, 0 - 1 \cdot 3, 1 - (-2) \cdot 3) = (0, -3, 7); \\ \underline{u} \leftarrow (1, 1, -2); \\ \underline{v} \leftarrow (0, -3, 7); \end{cases}$$

$$d = 1; \; \xi = -2; \; \eta = -2 \Rightarrow y^{-1} = 3^{-1} \, mod \, 7 \equiv_7 -\mathbf{2} \equiv_7 \mathbf{5}$$

3.2 Exercise 2

Consider the following field: $\mathbb{F}_{11} \cong \mathbb{Z}/11\mathbb{Z} \cong \mathbb{Z}_{11}$

1. *Find the number of primitive elements (i.e., generators of* $\mathbb{F}_{11}^*$*).*
2. *Compute the value of every primitive element.*
3. *List all subgroups of* $\mathbb{F}_{11}^*$ *together with their order.*
4. *Compute the multiplicative inverse of* $x = 7$*.*
5. *Describe the additive abelian group:* $< \mathbb{F}_{11}, + >$*.*

(1) Find the number of primitive elements (i.e., generators of $\mathbb{F}_{11}^*$*).*

$$\mathbb{F}_{11}^* = \{1, 2, \ldots, 10\};\ n = |\mathbb{F}_{11}^*| = 10;$$

$$\text{No. of generators} = \varphi(n) = \varphi(10) = \varphi(2 \cdot 5) = 4$$

equivalently,

$$\text{No. of generators} = |\{0 < i < n : gcd(i, n) = 1\}| = |\{1, 3, 7, 9\}| = 4.$$

(2) Compute the value of every primitive element.

Knowing the prime factorization of the group order $n = 2 \cdot 5$, we start from consider $g = 2$ as a possible group generator:
$2^2 \equiv_{11} 4$, $2^3 \equiv_{11} 8$, $2^4 \equiv_{11} 5$, $2^5 \equiv_{11} 10$, thus we conclude that $g_0 = g = 2$ is effectively a generator! The other 3 values are:

$g_1 = g_0^3 = 2^3 \equiv_{11} 8$;

$g_2 = g_0^7 = 2^7 \equiv_{11} 7$;

$g_3 = g_0^9 = 2^9 \equiv_{11} 6$.

In order to verify the above conclusions, you can list all the elements generated by g_3: $< g_3 >= \{g_3 = 6,\ g_3^2 = 3,\ g_3^3 = 7,\ g_3^4 = 9,\ g_3^5 = 10,\ g_3^6 = 5,\ g_3^7 = 8,\ g_3^8 = 4,\ g_3^9 = 2,\ g_3^{10} = 1\}$.

(3) List all subgroups of $\mathbb{F}_{11}^*$ *together with their order.*

$$\mathbb{F}_{11}^* = \{1, 2, \ldots, 10\};\ n = |\mathbb{F}_{11}^*| = 10$$

Knowing the prime factorization of the group order $n = 2 \cdot 5$, we can say that there exist only 2 proper subgroups H_1, H_2 with cardinality $n_1 = 2$ and $n_2 = 5$, respectively.
$H_1 =< h_1 >$ with h_1 element of $\mathbb{F}_{11}^*$ with order $n_1 = 2$, $h_1 = g_0^{n/n_1} \equiv_{11} 10$;
$H_2 =< h_2 >$ with h_2 element of $\mathbb{F}_{11}^*$ with order $n_2 = 5$, $h_2 = g_0^{n/n_2} \equiv_{11} 4$;
The subgroups of $\mathbb{F}_{11}^*$ are:

$H_0 = \{1\}$, $n_0 = 1$

$H_1 = \{10, 1\},\ n_1 = 2$

$H_2 = \{4, 5, 9, 3, 1\},\ n_2 = 5$

$\mathbb{F}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\},\ n = 10$

(3) Compute the multiplicative inverse of $x = 7$.

Employing the Euclidean Algorithm, we have:

$$p = 11,\ x = 7 \Rightarrow\ 1 = gcd(7, 4) = 7\xi + 4\eta \text{ dove } \xi = 2,\ \eta = -3 \Rightarrow x^{-1} \equiv_{11} \mathbf{8}$$

Analogously, through employing the group law and the S&M Left to Right exponentiation algorithm:

$$x^{-1} \equiv_{11} 7^9 \equiv_{11} 7^{1001_2} \equiv_{11} ((7^2)^2)^2 \cdot 7 \equiv_{11} (5^2)^2 \cdot 7 \equiv_{11} 3^2 \cdot 7 \equiv_{11} \mathbf{8}$$

(4) Describe the additive abelian group: $< \mathbb{F}_{11}, + >$.

$< \mathbb{F}_{11}, + >= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, $| < \mathbb{F}_{11}, + > | = 11$, is a cyclic group ($\cong \mathbb{Z}_{11}$) where all non-zero elements are generators (n.b., the group has a prime order) therefore, it does not have any proper subgroup.

No. of generators $= \varphi(11) = 10$

Taking $g = 10$ as a generator:

$$g \equiv_{11} 10,\ 2g \equiv_{11} 9,\ 3g \equiv_{11} 8$$
$$4g \equiv_{11} 7,\ 5g \equiv_{11} 6,\ 6g \equiv_{11} 5,$$
$$7g \equiv_{11} 4,\ 8g \equiv_{11} 3,\ 9g \equiv_{11} 2,$$
$$10g \equiv_{11} 1,\ 11g \equiv_{11} 0$$

3.3 Exercise 3

Consider: $\mathbb{F}_{13} \cong \mathbb{Z}/13\mathbb{Z} \cong \mathbb{Z}_{13}$, describe the multiplicative group of the field through listing all the subgroups (and their cardinality) and their generators. Show the relations among the subgroups.

Sol: n = 12, No. of subgroups = 6;

$n_0 = 1,\ H_0 =< 1 >= \{1\}$;

$n_1 = 4,\ H_1 =< 8 >=< 5 >= \{1, 5, 8, 12\}$;

$n_2 = 2,\ H_2 =< 12 >= \{1, 12\}$;

$n_3 = 3,\ H_3 =< 3 >=< 9 >= \{1, 3, 9\}$;

$n_4 = 6,\ H_4 =< 4 >=< 10 >= \{1, 3, 4, 9, 10, 12\}$;

$n_5 = 12,\ H_5 =< 2 >=< 6 >=< 7 >=< 11 >= \mathbb{F}_{13}^*$;

$H_0 < H_2 < H_1 < H_5; \quad H_0 < H_3 < H_4 < H_5.$

4 Exercises on fields $\mathbb{F}_{p^n}$

4.1 Exercise 1

Check whether the following polynomial $f(x) = x^2 - x - 1 \in \mathbb{F}_3[X]$ is irreducible or not. Subsequently, write the addition and multiplication tables of the field

$$\mathbb{F}_{3^2} \cong \mathbb{F}_3[X]/ < f(x) > \cong \mathbb{F}_3(\alpha) \text{ con } \alpha \in \mathbb{F}_{3^2} \backslash \mathbb{F}_3 : f(\alpha) = 0.$$

The polynomial $f(x) \in \mathbb{F}_3[X]$ does not have any root in $\mathbb{F}_3$ ($f(0) = 2$, $f(1) = 1$, $f(2) = 1$) therefore, being $deg(f(x)) = 2$, we can conclude that it is irreducible.

+	0	1	2	α	α+1	α+2	2α	2α+1	2α+2
0	0	1	2	α	α+1	2+α	2α	2α+1	2α+2
1	1	2	0	α+1	α+2	α	2α+1	2α+2	2α
2	2	0	1	α+2	α	α+1	2α+2	2α	2α+1
α	α	α+1	α+2	2α	2α+1	2α+2	0	1	2
α+1	α+1	α+2	α	2α+1	2α+2	2α	1	2	0
α+2	α+2	α	α+1	2α+2	2α	2α+1	2	0	1
2α	2α	2α+1	2α+2	0	1	2	α	α+1	α+2
2α+1	2α+1	2α+2	2α	1	2	3	α+1	α+2	α
2α+2	2α+2	2α	2α+1	2	0	1	α+2	α	α+1

·	1	2	α	α+1	α+2	2α	2α+1	2α+2
1	1	2	α	α+1	α+2	2α	2α+1	2α+2
2	2	1	2α	2α+2	2α+1	α	α+2	α+1
α	α	2α	α+1	2α+1	1	2α+2	2	α+2
α+1	α+1	2α+2	2α+1	2	α	α+2	2α	1
α+2	α+2	2α+1	1	α	2+2α	2	α+1	2α
2α	2α	α	2α+2	α+2	2	α+1	1	2α+1
2α+1	2α+1	α+2	2	2α	α+1	1	α+2	α
2α+2	2α+2	α+1	α+2	1	2α	2α+1	α	α+1

(1) Find the primitive elements of the field. Show all the possible irreducible polynomials; and show all the possible primitive polynomials.

$$\mathbb{F}_{3^2} \cong \mathbb{F}_3(\alpha) = \theta_0 + \alpha\theta_1 : \theta_0, \theta_1 \in \mathbb{F}_3; \alpha \in \mathbb{F}_{3^2} \backslash \mathbb{F}_3 : f(\alpha) = \alpha^2 - \alpha - 1 = 0.$$

No. of irreducible polynomial with degree equal to 2: $N_2(3) = (3^2 - 3)/2 = 3$; In order to find these three polynomial, considering the reduced elements in the field we proceed as follows: $f(x) = x^2 + \theta_1 x + \theta_0$; $f(0) \neq 0 \Rightarrow \theta_0 \neq 0 \Leftrightarrow \theta_0 = 1, 2$; we have two cases:
(1st case): $f(x) = x^2 + \theta_1 x + 1$, we need that: $f(2) = 2 + 2\theta_1 \neq 0 \Rightarrow \theta_1 \neq 2$; $f(1) = 2 + \theta_1 \neq 0 \Rightarrow \theta_1 \neq 1$; in such a way we have found the 1st irreducible polynomial:

$$f_1(x) = x^2 + 1$$

(2nd case): $f(x) = x^2 + \theta_1 x + 2$, we need that: $f(1) = \theta_1 \neq 0$; $f(2) = 6 + 2\theta_1 \neq 0 \Rightarrow \theta_1 \neq 0$; so, also the other two polynomials have been identified:

$$f_2(x) = x^2 + x + 2$$
$$f_3(x) = x^2 + 2x + 2 = x^2 - x - 1$$

Let $n = |\mathbb{F}_{3^2}^*|$ be the order of the multiplicative group. The number of primitive elements of the field is: $\varphi(n) = \varphi(8) = 4$;

the number of primitive polynomials with degree 2 and characteristic equal to 3 is: $M_2(3) = \varphi(8)/2 = 2$.

We previously found three irreducible polynomials: only two of these will be also primitive!
We start from finding a primitive element in $\mathbb{F}_{3^2}$, and employing the irreducible polynomial $f(x) = x^2 - x - 1$ to do the needed computations. Assume $\alpha \in \mathbb{F}_{3^2} \backslash \mathbb{F}_3$ as a root of $f(x)$, $(f(\alpha) = 0 \Leftrightarrow \alpha^2 = \alpha + 1)$.
we can easily verify that

$$\alpha^1 = \alpha;\ \alpha^2 = \alpha + 1;\ \alpha^3 = 2\alpha + 1;\ \alpha^4 = 2 \Rightarrow \alpha \text{ is primitive.}$$

(Obs.: the divisors of n are 1,2,4,8.)
Once a primitive element has been identified $\beta_0 = \alpha$, the other ones are easily computed: $\beta_1 = \alpha^3 = 2\alpha + 1$, $\beta_2 = \alpha^5 = 2\alpha$, $\beta_3 = \alpha^7 = \alpha + 2$.
In order to find the primitive polynomials, we can apply the definition:

$$g_1(x) = (x - \alpha)(x - \alpha^{3^1}) = x^2 + 2x + 2 = x^2 - x - 1$$
$$g_2(x) = (x - \beta_2)(x - \beta_2^{3^1}) = (x - \alpha^5)(x - \alpha^{15}) = x^2 + x + 2$$

4.2 Exercise 2

Describe the following finite field: $\mathbb{F}_{2^3}$.

Let $f(x)$ be the irreducible polynomial employed to represent $\mathbb{F}_{2^3}$: $\mathbb{F}_{2^3} \cong \mathbb{F}_2(\alpha) = \{\theta_0 + \alpha\theta_1 + \alpha^2\theta_2 : \theta_0, \theta_1, \theta_2 \in \mathbb{F}_2;\ f(\alpha) = 0\}$.

The No. of primitive elements $= \varphi(|\mathbb{F}_{2^3}^*|) = \varphi(7) = 6$, therefore, all elements $\neq 0, 1$ are generators of the multiplicative group.
No. of irreducible polynomial with degree $3 = N_3(2) = (2^3 - 2)/3 = 2$.
No. of irreducible polynomial with degree $3 = M_3(2) = \varphi(7)/3 = 2$. As it is expected, since every elements is a generator.
Being a cubic field extension, a necessary and sufficient condition for the polynomials to be irreducible is that they do not have any root in equal to either 0 or 1. In other words, the polynomials must have an odd number of non-zero coefficients with a constant term different from zero:

$$f_1(x) = x^3 + x^2 + 1; \qquad f_2(x) = x^3 + x + 1$$

4.3 Exercise 3

Describe the following finite field: $\mathbb{F}_{2^5}$.

No. of irreducible polynomials with degree $5 = N_5(2) = (2^5 - 2)/5 = 6$.
No. of primitive elements $= \varphi(|\mathbb{F}_{2^5}^*|) = \varphi(31) = 30$ therefore all elements $\neq 0, 1$ are generators; The number of irreducible polynomials is equal to No. of primitive ones.
In order to show the 6 primitive polynomials, we start listing all polynomials with three and five non-zero coefficients (including the constant term). (Necessary condition for the irreducibility is that such polynomials do not have roots in the base field $\mathbb{F}_2$):

$$
\begin{aligned}
f_1(x) &= x^5 + x^4 + x^3 + x^2 + 1 \\
f_2(x) &= x^5 + x^4 + x^3 + x + 1 \\
f_3(x) &= x^5 + x^4 + x^2 + x + 1 \\
f_4(x) &= x^5 + x^3 + x^2 + x + 1 \\
f_5(x) &= x^5 + x^4 + 1 \\
f_6(x) &= x^5 + x^3 + 1 \\
f_7(x) &= x^5 + x^2 + 1 \\
f_8(x) &= x^5 + x + 1
\end{aligned}
$$

Through applying the irreducibility test, we find that $f_5(x)$ and $f_8(x)$ are **reducible**.

4.4 Exercise 4

Consider the field $\mathbb{F}_{3^4} \cong \mathbb{F}_3[X]/ < f(x) >$:
(1) write the number of primitive elements;
(2) write the number of irreducible polynomials;
(3) write the number of primitive polynomials;
(4) Verify that $f(x) = x^4 + x - 1 \in \mathbb{F}_3[X]$ *is irreducible.*
(5) verify that $\alpha \in \mathbb{F}_{3^4} \backslash \mathbb{F}_3 \ : \ f(\alpha) = 0$ *is a primitive element of the field.*
(6) Knowing that $f(x) = (x - \alpha)(x - \alpha^3)(x - \alpha^9)(x - \alpha^{27}) = x^4 + x - 1$ *is primitive, find another primitive polynomial. (Hint: consider* $\beta = \alpha^7$*)*

Solution:
$n = 80$, *No. of primitive elements* $= 32$; *No. of irreducible polynomials* $= 18$; *No. of primitive polynomials = 8.*
Necessary condition for $f(x) = x^4 + x - 1$ *to be irreducible:* $f(0) = 2 \neq 0$, $f(1) = 1 \neq 0$, $f(2) = 2 \neq 0$, *therefore this polynomial cannot be divided by a linear factor with coefficients in* $\mathbb{F}_3$. *In addition, it is necessary to verify that the polynomial may not be decomposed as:*

$$(x^4 + x + 1) = (x^2 + ax + b)(x^2 + cx + d) \quad a, b, c, d \in \mathbb{F}_3$$

$$\begin{cases} a+c=0 \\ d+ac+b=0 \\ ad+bc=0 \\ bd=-1 \end{cases}$$

looking at both the first and the last equation we notice that the possible values for $a,b,c,d \in \mathbb{F}_3$ *are:* $a=1$, $d=-1$ *or* $a=-1$, $d=1$; *whilst* $a=1$, $c=-1$ *oppure* $a=-1$, $c=1$; *for each combination of these values we notice that the second equation does not hold. We can then conclude that* $f(x)=x^4+x-1 \in \mathbb{F}_3[X]$ *is irreducible.*
Now, through employing $f(x)=x^4+x-1$ *to do the computations, another primitive polynomial is:* $g(x)=x^4+x^3-x^2-x-1$.
Note that:

$$\begin{aligned} &\alpha^4=-\alpha+1; \\ &\alpha^5=-\alpha^2+\alpha \\ &\alpha^6=-\alpha^3+\alpha^2; \\ &\alpha^7=\alpha^3+\alpha-1 \\ &\alpha^8=\alpha^2+\alpha+1; \\ &\alpha^9=\alpha^3+\alpha^2+\alpha \\ &\alpha^{10}=\alpha^3+\alpha^2-\alpha+1 \\ &\alpha^{16}=-\alpha^3+\alpha-1 \\ &\alpha^{20}=-\alpha^3-\alpha^2+\alpha \\ &\alpha^{40}=2; \end{aligned}$$