PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

Mohamed Boudiaf University of M'sila
Faculty of Mathematics and Computer Science
Department of Mathematics

Master's thesis

Domaine : Mathematics and Informatics
Tract : Mathematics
Option : Algebra and Discrete Mathematics

Theme

Arithmetic of the ring $F_q[\varepsilon]$, $\varepsilon^n=0$, $n\geq 1$, $\varepsilon^{i+1}=\varepsilon^i$, $i=1,2,3$

Presented by :
Kouidri Sarah

Before the jury composed of :

Mihoubi.D	University of M'sila	**President**.
Ghadbane.N	University of M'sila	**Supervisor** .
Heboub.L	University of M'sila	**Examiner**.

University Year 2020/2021

Acknowledgements

Thanks to GOD almighty for the completion of this work. Only due to his blessings I could finish it.

I would like to express my deepest gratitude to my advisor, Mr: N.Ghadbane, for his invaluable advices and suggestions.

My thanks also ago to the jury members for the honor they have done me by accepting to judge this modest work.

I would like to thank my beloved parents for their encouragement who are so supportive to me throughout my life. My sisters, brothers deserve my wholehearted thanks as well, to all my friends and all people who have helped me during my study.

This work is only a begining of my journey.

thanks

Table of contents

Notations

$\mathbb{Z}$:	The integer numbers.
$(G, +)$:	The group.
$(R, +, .)$:	The ring.
$H \leq G$:	H is a subgroup of G.
1_R :	The identity element of R.
$R[x]$:	The ring of polynomials in x with coefficients in R.
I :	The ideal.
M :	The maximal ideal.
R/I :	The quotient ring of R mod I.
$\mathbb{F}_q$:	The finite field of cardinal q.

Introduction

The theory of ideals and quotient rings parallels the theory of normal subgroups and quotient groups. In the theory of groups, we can quotient out by a subgroup if and only if it is a normal subgroup, the analogue of this for rings are (two-sided) ideals.

One starts with a ring R and a two-sided ideal I in R, and constructs a new ring, the quotient ring R/I, whose elements are the cosets of I in R subject to special " $+$ " and " $\cdot$ " operations.

The most important example of a quotient ring is the ring of residues modulo n, the quotient ring of the ring of integers $\mathbb{Z}$ by the ideal $n\mathbb{Z}$. The elements of $\mathbb{Z}/n\mathbb{Z}$ can be assumed to be the numbers $\{0, ..., n-1\}$, where the sum and the product are defined as the remainders on diving the usual sum and product by n.

This thesis is organized as follows:
In chapter 1, we begin with some elementary material concerning the rings and fileds.
In chapte 2, we study the arithmetic operations in the quotient ring.
In chapter 3, we present some notes over the arithmetic operations in the Rings $\mathbb{F}_q[\varepsilon]$.

Chapter 1

Preliminaries

In this chapter, we recall some basic informations and concepts used in the following chapter.

1.1 Rings

Consider the set $\mathbb{Z}$ of integer numbers. It has two binary operations " $+$ " (addition) and "." (multiplication) compatible with each other:

$$a(b+c) = ab + ac, (b+c)a = ba + ca.$$

We will this example as a motivation for a formal description of these operations and their properties.

1.1.1 Group and Subgroup

Definition 1.1.1 (Group) *A group is a pair $(G, +)$, where G is a set and $+ : G \times G \to G$ is a map (written $(a, b) \to a + b$) such that:*

1. (Associativity) $(a + b) + c = a + (b + c)$.
2. (Existence of zero) There exists an element $0 \in A$ such that $a + 0 = 0 + a = a$, $a \in A$.
3. (Existence of negative) For any $a \in A$ there exists an element $b \in A$ such that $a+b = 0$.

It is denoted by $-a$.

Remark 1.1.1 *To check $(G, +)$ is a group, we check the:*

- G is a closed under $+$.

- G has an identity

.- Each element has an inverse.

Definition 1.1.2 (Abelain group) *A group $(G; +)$ is a said to be an abelian group, if " $+$ " is comumutative.*

Example 1.1.1 *The set of natural numbers $\mathbb{N} = \{1, 2, 3, ...\}$ has obvious addition operation. But it is not a group: it does not contain negatives of nonzero elements. For example $-1 \notin \mathbb{N}$.*

The following are examples of abelian groups.

(1) The set $\mathbb{Z}$ of integer numbers.

(2) The set $\mathbb{Q}$ of rational numbers.

(3) The set $\mathbb{R}$ of real numbers.

(4) The set $\mathbb{C}$ of complex numbers.

Definition 1.1.3 (Subgroup) *Let G be a group. A subset H of G is a subgroup of G if:*

(a) (Closure) H is closed under the group operation: If $a, b \in H$, then $a + b \in H$.

(b) (Identity) $1 \in H$.

(c) (Inverses) If $a \in H$, then $a^{-1} \in H$.

The notation $H < G$ means that H is a subgroup of G.

Example 1.1.2 *Let $n \in \mathbb{Z}$. Consider $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$. Show that $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$, the group of integers under addition. $n\mathbb{Z}$ consists of all multiples of n. First,we show that $n\mathbb{Z}$ is closed under addition. If $nx, ny \in n\mathbb{Z}$, then $nx + ny = n(x + y) \in n\mathbb{Z}$. Therefore,$n\mathbb{Z}$ is closed under addition. Next, the identity element of $\mathbb{Z}$ is 0. Now $0 = n.0$, so $0 \in n\mathbb{Z}$. Finally, suppose $nx \in \mathbb{Z}$. The additive inverse of nx in $\mathbb{Z}$ is $-nx$, and $-nx = n(-x)$. This is n times something, so it's in $n\mathbb{Z}$. Thus, $n\mathbb{Z}$ is closed under taking inverses. Therefore, $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.*

Definition 1.1.4 (Ring) *A ring is a triple $(R, +, \cdot)$, where R is a set and*
" $+$ " : $R \times R \to R$, " $\cdot$ " : $R \times R \to R$ are binary operations such that:

1. $(R;+)$ *is an abelian group.*

2. (Associativity of multiplication) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

3. (Existence of unity) $\exists 1_R \in R$ *such that* $a \cdot 1_R = 1_R \cdot a = a$ *for all* $a \in R$.

4. (Distributivity) $a \cdot (b + c) = a \cdot b + a \cdot c$, $(b + c) \cdot a = b \cdot a + b \cdot c$ *for all* $a, b, c \in R$.

Example 1.1.3 *(1) The sets* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ *are rings with respect to the natural operations of addition and multiplication. All of them are commutative.*

(2) The sets of polynomials $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$ *are commutative rings.*

(3) The set $M_n(\mathbb{R})$ *of* $n \times n$ *matrices with real coefficients is a ring. Addition and multiplication of matrices* $A = (a_{ij}), B = (b_{ij})$ *is given by:*

$A + B = (c_{ij}), c_{ij} = a_{ij} + b_{ij}$;

$AB = (d_{ij}), d_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$.

The zero element of this ring is the zero matrix. The unity element of this ring is the identity matrix.

$$\mathbf{I}_n = \begin{pmatrix} 1 & 0 & ... & 0 \\ 0 & 1 & ... & 0 \\ ... & ... & ... & ... \\ 0 & ... & ... & 1 \end{pmatrix}$$

Proposition 1.1.1 *Let* R *be a ring and let* a *and* b *be elements of* R. *Then,*

(1) $a0 = 0a = 0$.

(2) $a(-b) = (-a)b = -(ab)$.

Proof. Let $x = a0$. We have

$$\begin{aligned} x &= a0 = a(0 + 0) \\ &= a0 + a0 \\ &= x + x. \end{aligned}$$

Adding $-x$ to both sides, we get $x = 0$, which is (1).
Let $y = a(-b)$. We want to show that y is the additive inverse of ab,
that is we want to show that $y + ab = 0$. We have:

$$\begin{aligned} y + ab &= a(-b) + ab \\ &= a(-b + b) \\ &= a0 \\ &= 0, \end{aligned}$$

by (1). Hence (2). ■

Proposition 1.1.2 *Let R be a set that satisfies all the axioms of a ring, except possibly $a + b = b + a$. Then R is a ring.*

Proof. It suffices to prove that addition is commutative. We compute $(a + b)(1 + 1)$, in two different ways. Distributing on the right,

$$\begin{aligned} (a + b)(1 + 1) &= (a + b)1 + (a + b)1 \\ &= a + b + a + b \end{aligned}$$

On the other hand, distributing this product on the left we get

$$\begin{aligned} (a + b)(1 + 1) &= a(1 + 1) + b(1 + 1) \\ &= a + a + b + b. \end{aligned}$$

Thus

$$a + (b + a) + b = (a + b)(1 + 1) = a + a + b + b.$$

Cancelling an a on the left and a b on the right, we get

$$b + a = a + b,$$

which is what we want. Note the following identity. ■

Lemma 1.1.1 *Let R be a ring and let a and b be any two elements of R. Then*

$$(a+b)^2 = a^2 + ab + ba + b^2.$$

Proof. Easy application of the distributive laws. ■

Definition 1.1.5 (Commutative ring) *Let R be a ring. We say that R is commutative if the multiplication is commutative, that is $a.b = b.a$*

Definition 1.1.6 (Boolean ring) *Let R be a ring. We say that R is boolean if for every $a \in R, a^2 = a$.*

Proposition 1.1.3 *Every boolean ring is commutative.*

Proof. We compute $(a+b)^2$.

$$\begin{aligned} a+b &= (a+b)^2 \\ &= a^2 + ba + ab + b^2 \\ &= a + ba + ab + b. \end{aligned}$$

Cancelling we get $ab = -ba$. If we take $b = 1$, then $a = -a$, so that $-(ba) = (-b)a = ba$. Thus $ab = ba$. ■

Definition 1.1.7 (Division ring) *Let R be a ring. We say that R is a division ring if $R - \{0\}$ is a group under multiplication. If in addition R is commutative, we say that R is a field. Note that, a ring is a division ring if every non-zero element has a multiplicative inverse. Similary for commutative rings and fields.*

Example 1.1.4 *The following tower of subsets $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ is in fact a tower of subfields. Note that $\mathbb{Z}$ is not a field however, as 2 does not have a multiplicative inverse. Further the subring of $\mathbb{Q}$ given by those rational numbers with odd denominator is not a field either. Again 2 does not have a multiplicative inverse.*

Definition 1.1.8 (Zero-divisor ring) *Let R be a ring. We say that $a \in R$, $a \neq 0$, is a zero-divisor if there is an element $b \in R$, $b \neq 0$, such that, $ab = 0$ or $ba = 0$.*

Proposition 1.1.4 *If an element a has a multiplicative inverse in R, then a is not a zero divisor.*

Proof. Suppose that $ba = 0$ and that c is the multiplicative inverse of a. We compute bac in two different ways.

$$\begin{aligned} bac &= (ba)c \\ &= 0c \\ &= 0. \end{aligned}$$

On the other hand

$$\begin{aligned} bac &= (ba)c \\ &= b1 \\ &= b. \end{aligned}$$

Thus $b = bac = 0$. Thus a is not a zero divisor. ■

Definition 1.1.9 (Domain) *Let R be a ring. We say that R is a **domain** if R has no zero-divisors. If in addition R is commutative, then we say that R is an **integral domain**. Every division ring is a domain. Unfortunately the converse is not true.*

Example 1.1.5 *$\mathbb{Z}$ is an integral domain. In fact any subring of a division ring is clearly a domain. Many of the examples of rings that we have given are in fact not domains.*

1.2 Ring Homomorphisms

Definition 1.2.1 *Let $\varphi : R \to S$ be a function between two rings. We say that φ is a ring homomorphism if for every a and $b \in R$,*

$$\begin{aligned} \varphi(a+b) &= \varphi(a) + \varphi(b), \\ \varphi(a.b) &= \varphi(a).\varphi(b), \end{aligned}$$

and in addition $\varphi(1) = 1$.

Example 1.2.1 *Let* $f : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $f(n) = \overline{n}$, *the residue class of* n *mod* m. *Then* f *is a homomorphism.*

Remark 1.2.1 *Let* $\varphi : R \to S$ *be a ring homomorphism. The* ***kernel*** *of* φ, *denoted* $Ker\varphi$, *is the inverse image of zero. As in the case of groups, a very natural question arises. What can we say about the kernel of a ring homomorphism? Since a ring homomorphism is automatically a group homomorphism, it follows that the kernel is a normal subgroup. However since a ring is an abelian group under addition, in fact all subgroups are automatically normal.*

Definition 1.2.2 *Let* R *be a ring and let* I *be a subset of* R.
We say that I *is an ideal of* R *and write* $I \leq R$ *if* I *is a an additive subgroup of* R *and for every* $a \in I$ *and* $r \in R$, *we have* $ra \in I$ *and* $ar \in I$.

Proposition 1.2.1 *Let* $\varphi : R \to S$ *be a ring homorphism and let* I *be the kernel of* φ. *Then* I *is an ideal of* R.

Proof. We have already seen that I is an additive subgroup of R.

Suppose that $a \in I$ and $r \in R$. Then

$$\begin{aligned} \varphi(ra) &= \varphi(r)\varphi(a) \\ &= \varphi(r)0 \\ &= 0. \end{aligned}$$

Thus φ is in the kernel of φ. Similarly for ar. As before, given an additive subgroup H of R, we let R/H denote the group of left cosets of H in R. ■

Proposition 1.2.2 *Let* R *be a ring and let* I *be an ideal of* R, *such that* $I \neq R$. *Then* R/I *is a ring. Furthermore there is a natural ring homomorphism* $u : R \to R/I$ *which sends* r *to* $r + I$.

Theorem 1.2.1 *Let R be a ring and I an ideal not equal to all of R. Let $u : R \to R/I$ be the obvious map. Then u is universal amongst all ring homomorphisms whose kernel contains I. That is, suppose $\phi : R \to S$ is any ring homomorphism, whose kernel contains I. Then there is a unique ring homomomorphism $\psi : R/I \to S$.*

Theorem 1.2.2 *(Isomorphism Theorem) Let $\varphi : R \to S$ be a homomorphism of rings. Suppose that φ is onto and let I be the kernel of φ. Then S is isomorphic to R/I.*

Example 1.2.2 *Let $\psi : \mathbb{Q}[x]/(x^2-2) \to \mathbb{Q}\left(\sqrt[2]{2}\right)$ defined by $\psi(a_0 + b_0 x) = a_0 + b_0\sqrt[2]{2}$, ψ is an ismorphism and $\mathbb{Q}\left(\sqrt[2]{2}\right) \approxeq \mathbb{Q}[x]/(x^2-2)$.*

1.3 Polynomial Rings

Definition 1.3.1 *A polynomial of degree n over a ring R is an expression of the form*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0 = \sum_{i=0}^{n} a_i x^i;$$

where $a_i \in R$ and $a_n \neq 0$.

If R is a ring, the ring of polynomials in x with coefficients in R is denoted $R[x]$.

Proposition 1.3.1 *Let R be an integral domain. Then the units in $R[x]$ are precisely the units in R.*

Proof. One direction is clear. A unit in R is a unit in $R[x]$. Now suppose that $f(x)$ is a unit in $R[x]$. Given a polynomial g, denote by $d(g)$ the degree of $g(x)$ (note that we are not claiming that $R[x]$ is a Euclidean domain). Now $f(x)g(x) = 1$. Thus

$$\begin{aligned} 0 &= d(1) \\ &= d(fg) \\ &\geq d(f) + d(g). \end{aligned}$$

Thus both of f and g must have degree zero. It follows that $f(x) = f_0$ and that f_0 is a unit in R. ■

Proposition 1.3.2 *Let R be a ring. The natural inclusion*

$$R \to R[x]$$

which just sends an element $r \in R$ to the constant polynomial r, is a ring homomorphism.

Definition 1.3.2 *Let R be a ring and let α be an element of R. The natural ring homomorphism*
$\varphi : R[x] \to R$,
which acts as the identity on R and which sends x to α, is called evaluation at α and is often denoted ev_a. We say that α is a zero or root of $f(x)$, if $f(x)$ is in the kernel of ev_a.

1.4 Fields

Recall that a field is a commutative ring such that every its nonzero element is invertible. We know the fields $\mathbb{Q}; \mathbb{R}; \mathbb{C}$. Also we know that for any prime integer p, the quotient ring $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a field.

Proposition 1.4.1 *Let K be a field and let $p \in k[x]$ be an irreducible polynomial. Then $k[x]/(p)$ is a field.*

Proof. Let $f \in k[x]$ such that $\overline{f} \neq 0$ in $k[x]/(p)$. Then $f \notin (p)$. If $d = gcd(f; p)$ then $d \mid p$. Therefore $d = 1$ or $d = p$. If $d = p$ then $p \mid f$, a contradiction. If $d = 1$, then there exist $u; v \in k[x]$ such that $fu + pv = 1$. This implies in $k[x]/(p)$ that $\overline{f}\ \overline{u} = 1$, that is, $\overline{f}$ is invertible and $k[x]/(p)$ is a field. ■

Definition 1.4.1 *Let L be a field. A subset $K \subset L$ is called a subfield if it is a subring of L and if K equipped with an induced ring structure is a field. The field L is called a field extension of K.*

Remark 1.4.1 *Given a field K and a subset $S \subset K$, the intersection of all subfields of K that contain S is a subfield called a subfield generated by S. It is the minimal subfield that contains S. The subfield of K generated by $\varnothing$ (or by $\{0;1\}$) is called the prime subfield of K. It is the smallest subfield contained in K.*

Proposition 1.4.2 *Let K be a field and let α be an element of K. Then the kernel of ev_a is the ideal $\langle x - \alpha \rangle$.*

Proof. Denote by I the kernel of ev_a. Clearly $x - \alpha$ is in I. On the other hand, $K[x]$ is a Euclidean domain, and so it is certainly a **PID**. Thus I is principal. Suppose it is generated by f, so that $I = \langle f \rangle$. Then f divides $x - \alpha$. If f has degree one, then $x - \alpha$ must be an associate of f and the result follows. If f has degree zero, then it must be a constant. As f has a root at α, in fact this constant must be zero, a contradiction. ■

Example 1.4.1 *In a principal ideal domain, an ideal generated by an irreducible element is maximal. Now, if K is a field, then the polynomial ring $k[x]$ is a principal ideal domain. It follows that if $P \in k[x]$ is an irreducible polynomial (that is, a nonconstant polynomial that does not admit a factorization into terms of smaller degrees), then $k[x]/(P)$ is a field. It contains a copy of K in a natural way. This is a very general way of constructing fields. For instance, the complex numbers $\mathbb{C}$ can be constructed as $R[x]/(x^2 + 1)$.*

Proposition 1.4.3 *Let K be a field and let $f(x)$ be a polynomial of degree two or three. Then $f(x)$ is irreducible if and only if it has no roots in K.*

Proof. If $f(x)$ has a root in K, then $f(x) = g(x)h(x)$, where $g(x)$ has degree one, by **(1.3.3)**. As the degree of f is at least two, it follows that $h(x)$ has degree at least one. Thus $f(x)$ is not irreducible. Now suppose that $f(x)$ is not irreducible. Then $f(x) = g(x)h(x)$, where neither g nor h is a unit. Thus both g and h have degree at least one. As the sum of the degrees of g and h is at most three, the degree of f, it follows that one of g and h has degree one. Now apply **(1.3.3)**. ■

Example 1.4.2 *First consider the polynomial $x^2 + 1$. Over the real numbers this is irreducible. Indeed, if we replace x by any real number a, then a^2 is non-negative and so $a^2 + 1$*

cannot equal zero. On the other hand $\pm i$ is a root of x^2+1, as $i^2+1=0$. Thus x^2+1 is reducible over the complex numbers . Indeed $x^2+1=(x+i)(x-i)$. Thus an irreducible polynomial might well become reducible over a larger field.

Consider the polynomial x^2+x+1. Suppose we work over the field F_5. We need to check if the five elements of F_5 are roots or not. We have

$$\begin{aligned} 1^2+1+1 &= 3 \\ 2^2+2+1 &= 2 \\ 3^2+3+1 &= 3 \\ 4^2+4+1 &= 1 \end{aligned}$$

Thus x^2+x+1 is irreducible over F_5. Now consider what happens over the field with three elements F_3. Then 1 is a root of this polynomial.

As neither 0 or 2 are roots, we must have

$$x^2+x+1=(x-1)^2=(x+2)^2,$$

which is easy to check.

Chapter 2

Aritmetic Operations in The Quotient Ring

In this chapter we define the aritmetic operations in quotient ring and describe its properties.

2.1 The Ideals

Definition 2.1.1 *An ideal of a ring R is a non-empty subset I satisfying*

1. If $a; b \in I$, then $a + b \in I$.
2. If $a \in I$ and $r \in R$, then $rx \in I$ and $xr \in I$.

Definition 2.1.2 (Principal ideal) *Let R be a commutative ring and let $a \in R$ be an element of R. The set $I = \langle a \rangle = \{ra | r \in R\}$ is an ideal and any ideal of this form is called principal.*

Lemma 2.1.1 *Let R be a ring. We say that $u \in R$ is a unit, if u has a multiplicative inverse. Let I be an ideal of a ring R. If I contains a unit, then $I = R$.*

Proof. Suppose that $u \in I$ is a unit of R. Then $vu = 1$, for some $v \in R$.
It follows that

$$1 = vu \in I.$$

Pick $a \in R$. Then

$$a = a \cdot 1 \in I.$$

■

Definition 2.1.3 (Prime ideal) *Let R be a ring and let I be an ideal of R. We say that I is prime if whenever $ab \in I$ then either $a \in I$ or $b \in I$.*

Example 2.1.1 *Let $R = \mathbb{Z}$. Then every ideal in $\mathbb{Z}$ has the form $\langle n \rangle = n\mathbb{Z}$. It is not hard to see that I is prime if n is prime.*

Definition 2.1.4 (Maximal ideal) *Let I be an ideal. We say that I is maximal if for every ideal J, such that $I \subset J$, either $J = I$ or $J = R$.*

Proposition 2.1.1 *Let R be a commutative ring. Then R is a field if the only ideals are $\{0\}$ and R.*

Proof. We have already seen that if R is a field, then R contains no non-trivial ideals. Now suppose that R contains no non-trivial ideals and let $a \in R$. Suppose that $a = 0$ and let $I = (a)$. Then $I = \{0\}$. Thus $I = R$. But then $1 \in I$ and so $1 = ba$. Thus a is a unit and as a was arbitrary, R is a field. ■

Corollary 2.1.1 *Let R be a commutative ring. Then every maximal ideal is prime.*

2.2 Quotient Rings

Let R be a ring, and let I be a (two-sided) ideal. Considering just the operation of addition, R is a group and I is a subgroup. In fact, since R is an abelian group under addition, I is a normal subgroup, and the quotient group $\frac{R}{I}$ is defined. Addition of cosets is defined by adding coset representatives:

$$(a + I) + (b + I) = (a + b) + I.$$

The zero coset is $0 + I = I$, and the additive inverse of a coset is given by:

$$-(a + I) = (-a) + I.$$

However, R also comes with a multiplication, and it's natural to ask whether you can turn $\frac{R}{I}$ into a ring by multiplying coset representatives:

$$(a+I)(b+I) = ab+I.$$

I need to check that that this operation is well-defined, and that the ring axioms are satisfied. In fact, everything works, and you'll see in the proof that it depends on the fact that I is an ideal. Specifically, it depends on the fact that I is closed under multiplication by elements of R. By the way, I'll sometimes write "$\frac{R}{I}$" and sometimes "R/I"; they mean the same thing.

Theorem 2.2.1 *If I is a two-sided ideal in a ring R, then R/I has the structure of a ring under coset addition and multiplication.*

Proof. Suppose that I is a two-sided ideal in R. Let $r, s \in I$.

Coset addition is well-defined, because R is an abelian group and I a normal subgroup under addition. I proved that coset addition was well-defined when I constructed quotient groups. I need to show that coset multiplication is well-defined:

$$(r+I)(s+I) = rs+I.$$

As before, suppose that

$$r+I = r\prime+I, \text{ so } r = r\prime+a, a \in I$$

$$s+I = s\prime+I, \text{ so } s = s\prime+b, b \in I$$

Then

$$(r+I)(s+I) = rs+I = (r\prime+a)(s\prime+b)+I = r\prime s\prime+r\prime b+as\prime+ab+I = r\prime s\prime+I = (r\prime+I)(s\prime+I).$$

The next-to-last equality is derived as follows: $r\prime b + as\prime + ab \in I$, because I is an ideal; hence $r\prime b + as\prime + ab + I = I$. Note that this uses the multiplication axiom for an ideal; in a sense, it explains why the multiplication axiom requires that an ideal be closed under multiplication by ring elements on the left and right. Thus, coset multiplication is well-defined. Verification of the ring axioms is easy but tedious: It reduces to the axioms for R.

For instance, suppose I want to verify associativity of multiplication. Take $r, s, t \in R$. Then

$$((r+I)(s+I))(t+I) = (rs+I)(t+I) = (rs)t+I = r(st)+I = (r+I)(st+I) = (r+I)((s+I)(t+I)).$$

(Notice how I used associativity of multiplication in R in the middle of the proof.) The proofs of the other axioms are similar. ■

Example 2.2.1 *The set of even integers $\langle 2 \rangle = 2\mathbb{Z}$ is an ideal in $\mathbb{Z}$. Form the quotient ring $\frac{\mathbb{Z}}{2\mathbb{Z}}$. Construct the addition and multiplication tables for the quotient ring. Here are some cosets:*

$$2 + 2\mathbb{Z}, -15 + 2\mathbb{Z}, 841 + 2\mathbb{Z}.$$

But two cosets $a+2\mathbb{Z}$ and $b+2\mathbb{Z}$ are the same exactly when a and b differ by an even integer. Every even integer differs from 0 by an even integer. Every odd integer differs from 1 by an even intege. So there are really only two cosets (up to renaming): $0 + 2\mathbb{Z} = 2\mathbb{Z}$ and $1 + 2\mathbb{Z}$. Here are the addition and multiplication tables:

$+$	$0+2\mathbb{Z}$	$1+2\mathbb{Z}$
$0+2\mathbb{Z}$	$0+2\mathbb{Z}$	$1+2\mathbb{Z}$
$1+2\mathbb{Z}$	$1+2\mathbb{Z}$	$0+2\mathbb{Z}$

$\times$	$0+2\mathbb{Z}$	$1+2\mathbb{Z}$
$0+2\mathbb{Z}$	$0+2\mathbb{Z}$	$0+2\mathbb{Z}$
$1+2\mathbb{Z}$	$0+2\mathbb{Z}$	$1+2\mathbb{Z}$

Proposition 2.2.1 *Let R be a ring, and let I be an ideal*
(a) If R is a commutative ring, so is R/I.
(b) If R has a multiplicative identity 1, then $1 + I$ is a multiplicative identity for R/I. In this case, if $r \in R$ is a unit, then so is $r + I$, and $(r + I)^{-1} = r^{-1} + I$.

Proof. (a) Let $r + I, s + I \in R/I$. Since R is commutative,

$$(r + I)(s + I) = rs + I = sr + I = (s + I)(r + I).$$

Therefore, R/I is commutative.
(b) Suppose R has a multiplicative identity 1. Let $r \in R$. Then

$(r+I)(1+I) = r\cdot 1 + I = r + I$ and $(1+I)(r+I) = 1\cdot r + I = r + I$.

Therefore, $1 + I$ is the identity of R/I.

If $r \in R$ is a unit, then

$(r^{-1}+I)(r+I) = r^{-1}r + I = 1 + I$ and $(r+I)(r^{-1}+I) = rr^{-1} + I = 1 + I$.

Therefore, $(r+I)^{-1} = r^{-1} + I$. ■

Example 2.2.2 *$\mathbb{Z}_3[x]$ is the ring of polynomials with coefficients in $\mathbb{Z}_3$. Consider the ideal $\langle 2x^2 + x + 2\rangle$.*

(a) How many elements are in the quotient ring?

(b) Reduce the following product in $\frac{\mathbb{Z}_3[X]}{\langle 2x^2+x+2\rangle}$ to the form $(ax + b) + \langle 2x^2 + x + 2\rangle$:

$$(2x + 1 + \left\langle 2x^2 + x + 2\right\rangle).(x + 1 + \left\langle 2x^2 + x + 2\right\rangle).$$

(c) Find $[x + 2 + \langle 2x^2 + x + 2\rangle]^{-1}$ in $\frac{\mathbb{Z}_3[X]}{\langle 2x^2+x+2\rangle}$.

The ring $\frac{\mathbb{Z}_3[X]}{\langle 2x^2+x+2\rangle}$ is analogous to $\mathbb{Z}_n = \frac{\mathbb{Z}}{\langle n\rangle}$. In the case of $\mathbb{Z}_n$, you do computations mod n: To "simplify", you divide the result of a computation by the modulus n and take the remainder. In $\frac{\mathbb{Z}_3[X]}{\langle 2x^2+x+2\rangle}$, the polynomial $2x^2 + x + 2$ acts like the "modulus". To do computations in $\frac{\mathbb{Z}_3[X]}{\langle 2x^2+x+2\rangle}$, you divide the result of a computation by $2x^2 + x + 2$ and take the remainder.

(a) By the Division Algorithm, any $f(x) \in \mathbb{Z}_3[x]$ can be written as

$$f(x) = (2x^2 + x + 2)q(x) + r(x), \text{ where } \deg r(x) \leq \deg(2x^2 + x + 2)$$

This means that $r(x) = ax + b$, where $a, b \in \mathbb{Z}_3$. Then

$$f(x) + \left\langle 2x^2 + x + 2\right\rangle = (2x^2 + x + 2)q(x) + r(x) + \left\langle 2x^2 + x + 2\right\rangle = ax + b + \left\langle 2x^2 + x + 2\right\rangle$$

Since there are 3 choices for a and 3 choices for b, there are 9 cosets.

(b) First, multiply the coset representatives:

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

Dividing $2x^2+1$ *by* $2x^2+x+2$*, I get*

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

Then

$$2x^2+1+\langle 2x^2+x+2\rangle=[(2x^2+x+2)(1)+(2x+2)]+\langle 2x^2+x+2\rangle=2x+2+\langle 2x^2+x+2\rangle$$

(c) To find multiplicative inverses in $\mathbb{Z}_3$*, you use the Extended Euclidean Algorithm. The same idea works in quotient rings of polynomial rings.*

$2x^2+x+2$	$-$	$2x$
$x+2$	$2x$	1
2	$2x+1$	0

$$\begin{aligned}
(1)(2x^2+x+2)-(2x)(x+2) &= 2\\
(1)(2x^2+x+2)+(x)(x+2) &= 2\\
(2)(2x^2+x+2)+(2x)(x+2) &= 1\\
(2)(2x^2+x+2)+(2x)(x+2)+\langle 2x^2+x+2\rangle &= 1+\langle 2x^2+x+2\rangle\\
(2x)(x+2)+\langle 2x^2+x+2\rangle &= 1+\langle 2x^2+x+2\rangle
\end{aligned}$$

Thus,

$$[x+2+\langle 2x^2+x+2\rangle]^{-1}=2x+\langle 2x^2+x+2\rangle$$

Proposition 2.2.2 *Let* R *be a ring and let* I *be an ideal of* R*. Then* R/I *is a domain if and only if* I *is prime.*

Proof. Suppose that I is prime. Let x and y be two elements of R/I. Then there are elements a and b of R such that $x=a+I$ and $y=b+I$. Suppose that $xy=0$, but that $x=0$, that is, suppose that $a\in I$.

$$\begin{aligned}
xy &= (a+I)(b+I)\\
&= ab+I\\
&= 0.
\end{aligned}$$

But then $ab \in I$ and as I is prime, $b \in I$. But then $y = b + I = I = 0$. Thus R/I is an domain.

Now suppose that R/I is a domain. Let a and b be two elements of R such that $ab \in I$ and suppose that $a \notin I$. Let $x = a + I$, $y = b + I$. Then $xy = ab + I = 0$. As $x = 0$, and R/I is an domain, $y = 0$. But then $b \in I$ and so I is prime. ■

Theorem 2.2.2 *Let R be a commutative ring. Then R/M is a field if M is a maximal ideal.*

Proof. Note that there is an obvious correspondence between the ideals of R/M and ideals of R that contain M.

The result therefore follows immediately from **(2.2.1)**. ■

Chapter 3

Aritmetic Operations of The Rings $\mathbb{F}_q[\varepsilon]$

In the last chapter, we define the ring $\mathbb{F}_q[\varepsilon]$ and give examples of the it.

3.1 The Ring $\mathbb{F}_q[\varepsilon], \varepsilon^2 = 0$

Definition 3.1.1 *Let p be a prime number, q be a bower of p. We consider the finite field of cardinal q, denoted $\mathbb{F}_q$. And we denote $\mathbb{F}_q[\varepsilon], \varepsilon^2 = 0$ the ring $\frac{\mathbb{F}_q[X]}{\langle X^2 \rangle}$. In other words, we have:*

$$\mathbb{F}_q[\varepsilon] = \{a + b\varepsilon : a, b \in \mathbb{F}_q, \varepsilon^2 = 0\}$$

Example 3.1.1 *We consider the finite field of cardinal 3. Where $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$*

$$\mathbb{Z}/3\mathbb{Z} = \{\overline{0}; \overline{1}; \overline{2}\}$$

Let $a, b \in \mathbb{F}_3$ we have for example $1 + 2\varepsilon \in \mathbb{F}_3[\varepsilon]$.

Definition 3.1.2 *the arithmetic operations in $\mathbb{F}_q[\varepsilon]$ can be decomposed into operations in $\mathbb{F}_q$ and they are computed as follows:*

$$X + Y = (x_0 + y_0) + (x_1 + y_1)\varepsilon$$

and

$$X \cdot Y = (x_0 y_0) + (x_0 y_1 + x_1 y_0)\varepsilon$$

Where $X = x_0 + x_1\varepsilon$ and $Y = y_0 + y_1\varepsilon$.

Example 3.1.2 *We consider the finite field of cardinal* 3. *Where* $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$:
Let $X = 1 + 2\varepsilon$ *and* $Y = 2 - \varepsilon$, *we have:*

$$\begin{aligned} X + Y &= (1+2) + (2-1)\varepsilon \\ &= \varepsilon \end{aligned}$$

and

$$\begin{aligned} X \cdot Y &= (1 \times 2) + (1 \times (-1) + 2 \times 2)\varepsilon \\ &= 2 + 3\varepsilon \\ &= 2 \end{aligned}$$

Proposition 3.1.1 *The non-invertible elements of* $\mathbb{F}_q[\varepsilon]$ *are the* $k\varepsilon$ *with* k *in* $\mathbb{F}_q$, *and for* a *and* b *in* $\mathbb{F}_q$ *with* $a \neq 0$, *we have:*

$$(a + b\varepsilon)^{-1} = a^{-1} - ba^{-2}\varepsilon.$$

Proof. For a and b in $\mathbb{F}_q$ with $a \neq 0$, we have:

$$(a + b\varepsilon)(a^{-1} - ba^{-2}\varepsilon) = 1.$$

Moreover, an element of $\mathbb{F}_q[\varepsilon]$ written in the form $a + b\varepsilon$ with a and b in $\mathbb{F}_q$ is invertible if and only if a is non-zero. ■

Example 3.1.3 *In the previous example we have*

$$\begin{aligned}(1+2\varepsilon)^{-1} &= 1^{-1} - 2.1^{-2}\varepsilon \\ &= 1 - 2\varepsilon\end{aligned}$$

Proposition 3.1.2 *The ring $\mathbb{F}_q[\varepsilon]$ admits $(\varepsilon) = \varepsilon\mathbb{F}_q$ for maximal ideal.*

Proof. For a, b and k in $\mathbb{F}_q$, we have:

$$k\varepsilon(a + b\varepsilon) = ak\varepsilon$$

So, we have: $(\varepsilon)\mathbb{F}_q[\varepsilon] \subset (\varepsilon)$; and (ε) is an ideal.

Moreover, the quotient ring is a field because for a and b in $\mathbb{F}_q$, $a + b\varepsilon$ can be represented by a and:

$$\frac{\mathbb{F}_q[\varepsilon]}{(\varepsilon)} = \mathbb{F}_q$$

So (ε) is a maximal ideal. ■

The ring $\mathbb{F}_q[\varepsilon]$ therefore has the property of being a local ring, as indicated by **Lemma 3.1.1**

Lemma 3.1.1 *The ring $\mathbb{F}_q[\varepsilon]$ is a local ring of residual field $\mathbb{F}_q$.*

Proof. By **Prposition 3.1.1 and 3.1.2**, the set of non-invertible elements of $\mathbb{F}_q[\varepsilon]$ is a maximal ideal of residual field $\mathbb{F}_q$. So the ring $\mathbb{F}_q[\varepsilon]$ is a local ring. ■

Proposition 3.1.3 *The ring $\mathbb{F}_q[\varepsilon]$ is an $\mathbb{F}_q$-vector space of dimension 2 of base $(1, \varepsilon)$; is :*

$$\mathbb{F}_q[\varepsilon] = \mathbb{F}_q + \mathbb{F}_q\varepsilon.$$

Proof. For a, a_0, b, b_0 and k in $\mathbb{F}_q$, we have:

$$a + b\varepsilon + a_0 + b_0\varepsilon = (a + a_0) + (b + b_0)\varepsilon$$

$$k(a + b\varepsilon) = ka + kb\varepsilon.$$

■

3.2 The Ring $\mathbb{F}_q[\varepsilon], \varepsilon^3 = \varepsilon^2$

Definition 3.2.1 *$\mathbb{F}_q$ is a finite field of order $q = p^d$ where d is a positive integer and p is a prime number. The ring $\mathbb{F}_q[\varepsilon]$; $\varepsilon^3 = \varepsilon^2$ can be constructed as an extension of the ring $\mathbb{F}_q$ by using the quotient ring of $\mathbb{F}_q[X]$ by the polynomial $X^3 - X^2$. An element $X \in \mathbb{F}_q[\varepsilon]$ is represented by $X = x_0 + x_1\varepsilon + x_2\varepsilon^2$ where $(x_0; x_1; x_2) \in \mathbb{F}_q^3$.*

Definition 3.2.2 *the arithmetic operations in $\mathbb{F}_q[\varepsilon]$ can be decomposed into operations in $\mathbb{F}_q$ and they are computed as follows:*

$$X + Y = (x_0 + y_0) + (x_1 + y_1)\varepsilon + (x_2 + y_2)\varepsilon^2$$

and

$$XY = (x_0y_0) + (x_0y_1 + x_1y_0)\varepsilon + [x_2y_0 + (x_1 + x_2)y_1 + (x_0 + x_1 + x_2)y_2]\varepsilon^2;$$

Where $X = x_0 + x_1\varepsilon + x_2\varepsilon^2$ and $Y = y_0 + y_1\varepsilon + y_2\varepsilon^2$.

Example 3.2.1 *Let $X; Y \in \mathbb{F}_5[\varepsilon]$, $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$ we have:*

$$\begin{aligned} X &= 1 + 4\varepsilon + 2\varepsilon^2 \\ Y &= 3 - 2\varepsilon + \varepsilon^2 \end{aligned}$$

then

$$\begin{aligned} X + Y &= (1 + 3\varepsilon - 2\varepsilon^2) + (3 - 2\varepsilon + \varepsilon^2) \\ &= (1 + 3) + (4 - 2)\varepsilon + (-2 + 1)\varepsilon^2 \\ &= 4 + 2\varepsilon - 2\varepsilon^2 \\ &= 4 + 2\varepsilon + 3\varepsilon^2 \end{aligned}$$

and

$$\begin{aligned} X \cdot Y &= (1 + 3\varepsilon - 2\varepsilon^2) \cdot (3 - 2\varepsilon + \varepsilon^2) \\ &= (1 \times 3) + (1 \times (-2) + 3 \times 3)\varepsilon + [(-2) \times 3 + (3 + (-2)) \times (-2) + (1 + 3 + (-2)) \times 1]\varepsilon^2 \\ &= 3 + (-2 + 9)\varepsilon + (-6 - 2 + 2)\varepsilon^2 \\ &= 3 + 2\varepsilon + 4\varepsilon^2 \end{aligned}$$

Proposition 3.2.1 *$\mathbb{F}_q[\varepsilon]$ is a vector space over $\mathbb{F}_q$ of dimension 3 and $\{1; \varepsilon; \varepsilon^2\}$ is it's basis.*

Proposition 3.2.2 *The product law in $\mathbb{F}_q[\varepsilon]$ can be written as:*

$$X \cdot Y = x_0y_0 + \delta_{XY}\varepsilon + ((x_0 + x_1 + x_2)(y_0 + y_1 + y_2) - x_0y_0 - \delta_{XY})\varepsilon^2;$$

where

$$\delta_{XY} = (x_0 + x_1)(y_0 + y_1 - x_0y_0 - x_1y_1 = x_0y_1 + x_1y_0.$$

Proof. We have:

$$(x_0 + x_1 + x_2)(y_0 + y_1 + y_2)) - x_0y_0 - \delta_{XY} = x_2y_0 + (x_1 + x_2)y_1 + (x_0 + x_1 + x_2)y_2 :$$

■

Corollary 3.2.1 *Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 \in \mathbb{F}_q[\varepsilon]$. We have:*

$$X^2 = x_0^2 + \delta_{X^2}\varepsilon + ((x_0 + x_1 + x_2)^2 - (x_0 + x_1)^2 + x_1^2)\varepsilon^2$$

and

$$X^3 = x_0^3 + \delta_{X^3}\varepsilon + ((x_0 + x_1 + x_2)^3 - (x_0 + x_1)^3 + x_1^3 + 3x_0^2x_1)\varepsilon^2$$

where:

$$\delta_{X^2} = (x_0 + x_1)^2 - x_0^2 - x_1^2 \ \ and \ \ \delta_{X^3} = (x_0 + x_1)^3 - x_0^3 - x_1^3 - 3x_0x_1^2.$$

The next proposition characterize the set $(\mathbb{F}_q[\varepsilon])^\times$ of invertible elements in $\mathbb{F}_q[\varepsilon]$.

Proposition 3.2.3 *Let $X = x_0 + x_1\varepsilon + x_2e^2 \in \mathbb{F}_q[\varepsilon]$. X is invertible if and only if x_0 and $x_0 + x_1 + x_2$ are invertible in $\mathbb{F}_q$. The inverse of X is given by:*

$$X^{-1} = x_0^{-1} - x_0x_1\varepsilon + ((x_0 + x_1 + x_2)^{-1} + x_0x_1^{-2} - x_0^{-1})\varepsilon^2$$

Proof. Let $X = x_0 + x_1\varepsilon + x_2e^2$ and $Y = y_0 + y_1\varepsilon + y_2\varepsilon^2$ be two elements of $\mathbb{F}_q[\varepsilon]$.

We have $X \cdot Y = x_0y_0 + \delta_{XY}\varepsilon + ((x_0 + x_1 + x_2)(y_0 + y_1 + y_2) - x_0y_0 - \delta_{XY})\varepsilon^2$

where $\delta_{XY} = x_0y_1 + x_1y_0$ then:

$$X \cdot Y = 1 \text{ if and only if } \begin{cases} x_0y_0 = 1 \\ \delta_{XY} = 0 \\ (x_0 + x_1 + x_2)(y_0 + y_1 + y_2) - x_0y_0 - \delta_{XY} = 0 \end{cases}$$

$$\text{if and only if } \begin{cases} x_0y_0 = 1 \\ x_0y_1 + x_1y_0 = 0 \\ (x_0 + x_1 + x_2)(y_0 + y_1 + y_2) = 1 \end{cases}$$

$$\text{if and only if } \begin{cases} y_0 = x_0^{-1} \\ y_1 = -x_1x_0^{-2} \\ y_2 = (x_0 + x_1 + x_2)^{-1}x + x_1x_0^{-2} - x_0^{-1} \end{cases}$$

So $X \in (\mathbb{F}_q[\varepsilon])$ if and only if $x_0 \neq 0$ and $x_0 + x_1 + x_2 \neq 0$: In this case we have:

$$X^{-1} = x_0^{-1} - x_0x_1\varepsilon + ((x_0 + x_1 + x_2)^{-1} + x_0x_1^{-2} - x_0^{-1})\varepsilon^2$$

■

Example 3.2.2 *Let $X = 1+2\varepsilon-2e^2 \in \mathbb{F}_3[\varepsilon]$. X is invertible if and only if x_0 and $x_0+x_1+x_2$ are invertible in $\mathbb{F}_3$. The inverse of X is given by:*

$$\begin{aligned} X^{-1} &= 1^{-1} - (1 \times 2)\varepsilon + ((1 + 2 - 2)^{-1} + 1 \times 2^{-2} - 1^{-1})\varepsilon^2 \\ &= 1 - 2\varepsilon + (1 + 3^2 - 1)\varepsilon^2 \\ &= 1 - 2\varepsilon \end{aligned}$$

Corollary 3.2.2 *Let $X \in \mathbb{F}_q[\varepsilon]$; then X is not invertible if and only if $X = x\varepsilon + y\varepsilon^2$ or $X = x + y\varepsilon - (x + y)\varepsilon^2$ where $(x; y) \in \mathbb{F}_q^2$. Now, we consider the set $I \cup J$ of non invertible elements in $\mathbb{F}_q[\varepsilon]$ where I and J are two ideals of $\mathbb{F}_q[\varepsilon]$ de ned by:*

$$I = \{x\varepsilon + y\varepsilon^2 \setminus (x; y) \in \mathbb{F}_q^2\} \text{ and } J = \{x + y\varepsilon - (x + y)\varepsilon^2 \setminus (x; y) \in \mathbb{F}_q^2\}$$

We have $I \cup J = \{x\varepsilon - x\varepsilon^2 \setminus x \in \mathbb{F}_q\}$, so $I \subset J$ is not an ideal, then we have the following Lemmas:

Lemma 3.2.1 *$\mathbb{F}_q[\varepsilon]$ is a non local ring.*

Definition 3.2.3 *We consider the canonical projection π_0 and π_1 defined by:*

$$\begin{array}{rcl} \pi_0 & : & \mathbb{F}_q[\varepsilon] \to \mathbb{F}_q \\ X & \to & x_0 \end{array}$$

And

$$\begin{array}{rcl} \pi_1 & : & \mathbb{F}_q[\varepsilon] \to \mathbb{F}_q \\ X & \to & x_1 \end{array}$$

Proposition 3.2.4 *π_0 and π_1 are two surjective morphisms of rings.*

Proof. From the definition of the sum and product law in $\mathbb{F}_q[\varepsilon]$, we have:

- $\pi_0(X+Y) = x_0 + y_0 = \pi_0(X) + \pi_0(Y)$ and $\pi_0(XY) = x_0y_0 = \pi_0(X)\pi_0(Y)$,so π_0 is a morphism of rings.

- $\pi_1(X+Y) = x_0+y_0+x_1+y_1+x_2+y_2 = (x_0 + x_1 + x_3)+(y_0 + y_1 + y_3) = \pi_1(X)+\pi_1(Y)$ and $\pi_1(X \cdot Y) = (x_0 + x_1 + x_3)(y_0 + y_1 + y_3) = \pi_1(X) \cdot \pi_1(Y)$,so π_1 is a morphism of rings.

Finally, for all $x \in \mathbb{F}_q \subset \mathbb{F}_q[\varepsilon]$, we have $\pi_0(x) = \pi_1(x) = x$, so π_0 and π_1 are two surjective morphisms. ■

3.3 The Ring $\mathbb{F}_q[\varepsilon], \varepsilon^4 = 0$

Definition 3.3.1 *$\mathbb{F}_q$ is a finite field of order $q = p^d$ where d is a positive integer and p is a prime number. The ring $\mathbb{F}_q[\varepsilon]$; $\varepsilon^4 = 0$ can be constructed as an extension of the ring $\mathbb{F}_q$ by using the quotient ring of $\mathbb{F}_q[X]$ by the polynomial X^4. An element $X \in \mathbb{F}_q[\varepsilon]$ is represented by $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ where $(x_0; x_1; x_2, x_3) \in \mathbb{F}_q^4$.*

Definition 3.3.2 *The arithmetic operations in $\mathbb{F}_q[\varepsilon]$ can be decomposed into operations in $\mathbb{F}_q$ and they are computed as follows:*

$$X + Y = (x_0 + y_0) + (x_1 + y_1)\varepsilon + (x_2 + y_2)\varepsilon^2 + (x_3 + y_3)\varepsilon^3$$

and

$$X \cdot Y = (x_0y_0) + (x_0y_1 + x_1y_0)\varepsilon + (x_0y_2 + x_1y_1 + x_2y_0)\varepsilon^2 + (x_0y_3 + x_1y_2 + x_2y_0 + x_2y_1 + x_3y_0)\varepsilon^3;$$

where $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ and $Y = y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$:

Example 3.3.1 *Let $X; Y \in \mathbb{F}_3[\varepsilon]$,we have:*

$$\begin{aligned} X &= 1 + 2\varepsilon + \varepsilon^2 + \varepsilon^3 \\ Y &= 1 - 2\varepsilon + \varepsilon^2 - \varepsilon^3 \end{aligned}$$

then

$$\begin{aligned} X + Y &= (1 + 2\varepsilon + \varepsilon^2 + \varepsilon^3) + (1 - 2\varepsilon + \varepsilon^2 - \varepsilon^3) \\ &= (1 + 1) + (2 - 2)\varepsilon + (1 + 1)\varepsilon^2 + (1 - 1)\varepsilon^3 \\ &= 2 + 2\varepsilon^2 \end{aligned}$$

$$\begin{aligned} X \cdot Y &= (1 + 2\varepsilon + \varepsilon^2 + \varepsilon^3) \cdot (1 - 2\varepsilon + \varepsilon^2 - \varepsilon^3) \\ &= (1 \times 1) + (1 \times (-2) + 2 \times 1)\varepsilon + (1 \times 1 + 2 \times (-2) + 1 \times 1)\varepsilon^2 \\ &\quad + (1 \times 1 + 2 \times 1 + 1 \times (-2) + 1 \times (-2) + 1 \times 1)\varepsilon^3 \\ &= 1 - 2\varepsilon^2 \end{aligned}$$

Proposition 3.3.1 *Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ is invertible in $\mathbb{F}_q$. if and only if x_0 and $x_0 + x_1 + x_2 + x_3$ are invertible in $\mathbb{F}_q$. The inverse of X is given by:*

$$\begin{aligned} X^{-1} &= x_0^{-1} - x_0^{-2}x_1\varepsilon + (-x_0^{-2}x_2 + x_0^{-3}x_1^2)\varepsilon^2 - x_0^{-1}(x_0^{-1}x_3 + x_0^{-2}x_1x_2 + [-x_0^{-1}(x_0^{-1}x_2 - x_0^{-2}x_1)]x_1)\varepsilon^3 \\ &= x_0^{-1} - x_0^{-2}x_1\varepsilon + (-x_0^{-2}x_2 + x_0^{-3}x_1^2)\varepsilon^2 - x_0^{-1}(x_0^{-1}x_3 + x_0^{-2}x_1x_2 - x_0^{-2}x_1x_2 + x_0^{-2}x_1^2)\varepsilon^3 \\ &= x_0^{-1} - x_0^{-2}x_1\varepsilon + (-x_0^{-2}x_2 + x_0^{-3}x_1^2)\varepsilon^2 - (x_0^{-2}x_3 + x_0^{-3}x_1x_2 - x_0^{-3}x_1x_2 + x_0^{-3}x_1^2)\varepsilon^3 \end{aligned}$$

Proposition 3.3.2 *$\mathbb{F}_q[\varepsilon]$ is a vector space over $\mathbb{F}_q$ of dimension 4 and $\{1; \varepsilon; \varepsilon^2; \varepsilon^3\}$ is it's basis.*

3.4 The Ring $\mathbb{F}_{2^d}[\varepsilon], \varepsilon^n = 0$

Definition 3.4.1 *Let d be an integer and n be an integer such that $n \geq 1$. We consider the quotient ring $A_n = \frac{\mathbb{F}_{2^d}[X]}{X^n}$, where $\mathbb{F}_{2^d}$ is the finite*

field of order 2^d. Then the ring A_n is identified to the finite ring $\mathbb{F}_{2^d}[\varepsilon]$ where $\varepsilon^n = 0$, i.e; :

$$A_n = \left\{ \sum_{i=0}^{n-1} a_i \varepsilon^i, a_i \in \mathbb{F}_{2^d}, 0 \leq i \leq n-1, \varepsilon^n = 0 \right\}$$

Definition 3.4.2 *Let $X = \sum_{i=0}^{n-1} x_i \varepsilon^i$ and $Y = \sum_{i=0}^{n-1} y_i \varepsilon^i$ we have $XY = \sum_{j=0}^{n-1} z_j \varepsilon^j$, where $z_j = \sum_{i=0}^{j} x_i y_{j-i}$.*

Proposition 3.4.1 *The elements non invertible in the ring A_n is the elements of ideal εA_n.*

Proof. See [1] ■

Remark 3.4.1 *Let $Y = \sum_{i=0}^{n-1} y_i \varepsilon^i$, be the inverse of the element $X = \sum_{i=0}^{n-1} x_i \varepsilon^i$, then*

$$\begin{cases} y_0 = x_0^{-1} \\ y_j = -x_0^{-1} \sum_{i=0}^{j-1} y_i x_{j-i} \end{cases}$$

Proposition 3.4.2 *A_n is a local ring of residuel field $\mathbb{F}_{2^d}$.*

Proof. Use the **Proposition 3.4.1** and **Definition 3.4.1** ■

Proposition 3.4.3 *A_n is a vectoriel-space over $\mathbb{F}_{2^d}$ of dimension n and bases $B = \{1; \varepsilon; \varepsilon^2; ...; \varepsilon^{n-1}\}$.*

Definition 3.4.3 *We consider the canonical projection π defined by:*

$$\begin{aligned} \pi &: A_n \to \mathbf{F}_{2^d} \\ X &= \sum_{i=0}^{n-1} x_i \varepsilon^i \to x_0 \end{aligned}$$

Proposition 3.4.4 *π is a morphism of rings.*

Proof. Let $X = \sum_{i=0}^{n-1} x_i\varepsilon^i$ and $Y = \sum_{i=0}^{n-1} y_i\varepsilon^i$, we are

$$\begin{aligned} XY &= \sum_{j=0}^{n-1} z_j\varepsilon^j \text{ where } z_j = \sum_{i=0}^{j} x_i y_{j-i} \text{ and} \\ X+Y &= \sum_{i=0}^{n-1}(x_i+y_i)\varepsilon^i \text{ so:} \\ \pi(X+Y) &= x_0+y_0 = \pi(X)+\pi(Y) \\ \pi(XY) &= z_0 = x_0y_0 = \pi(X).\pi(Y) \end{aligned}$$

■

Remark 3.4.2 *We denote $I_j = (\varepsilon^j)$, where $j = 1, ..., n-1$. Then, $(I_j)_{1\leq j\leq n-1}$ is a decreasing sequence of ideals of A_n and $I_1 = M_n$.*

$$M_n = I_1 \supseteq I_2 \supseteq ... \supseteq I_{n-1}$$

Lemma 3.4.1 $A_{n-1} \backsimeq A_n/I_{n-1}$.

Proof. Let $A_{n-1} = \left\{\sum_{i=0}^{n-2} x_i\delta^i \setminus x_i \in \mathbb{F}_{2^d}, 0 \leq i \leq n-1 \text{ and } \delta^{n-1} = 0\right\}$ and h the map defined as follows:

$$h : A_{n-1} \to \frac{A_n}{I_{n-1}}$$

$$\sum_{i=0}^{n-2} x_i\delta^i \to \sum_{i=0}^{n-2} x_i\varepsilon^i + I_{n-1}$$

Let $X = \sum_{i=0}^{n-2} x_i\varepsilon^i \in A_{n-1}$ prove that h is an isomorphism of rings.

- Let $A_{n-1}$and $Y = \sum_{i=0}^{n-1} y_i\varepsilon^i \in A_n$, we have $X+Y = \sum_{i=0}^{n-2}(x_i+y_i)\varepsilon^i \in A_{n-1}$ and $XY = \sum_{i=0}^{n-2} z_i\varepsilon^i \in A_{n-1}$ where, $z_j = \sum_{i=0}^{n-1} x_iy_{j-1}$ then, $h(X+Y) = h(X)+h(Y)$ and, $h(XY) = h(X)h(Y)$ and so, h is a homomorphism of rings.

- Let $X = \sum_{i=0}^{n-2} x_i\varepsilon^i \in A_{n-1}$ such that $h(X) = 0 + I_{n-1}$. Then, $\sum_{i=0}^{n-2} x_i\varepsilon^i + I_{n-1} = 0 + I_{n-1}$, $\sum_{i=0}^{n-2} x_i\varepsilon^i \in I_{n-1}$ so ,this means that $x_i = 0$ for all $i = 0, ..., n-2$. So $X = 0$, and $\ker h = 0$, this prove that h is injective. Now let $Y = \sum_{i=0}^{n-2} x_i\varepsilon^i + I_{n-1} \in A_n/I_{n-1}$, then we denote $X = \sum_{i=0}^{n-2} x_i\varepsilon^i$; we have $X \in A_{n-1}$ and $h(X) = Y$, so h is surjective.

Finally h is an isomorphism of rings. ■

Remark 3.4.3 *1). For all X in A_n, we denote $\overline{X} = X + I_{n-1}$ then, from **Lemma 3.4.1**:* $A_{n-1} = \{\overline{X} \mid X \in A_n\}$

2). Since $(I_k)_{k=1\ldots n-1}$ is a decreasing sequence of ideals of A_n, then $(I_k/I_{n-1})_{k=1\ldots n-1}$ is a decreasing sequence of ideals of A_{n-1}.

3). $M_{n-1} \simeq M_n/I_{n-1}$.

Corollary 3.4.1 *Let π_n the homomorphism defined by:*

$$\begin{array}{rcl} \pi_n & : & A_n \to A_{n-1} \\ X & \to & \overline{X} \end{array}$$

$\pi_n$is a surjective morphism of rings.

Since $A_n = F_{2^d}[X]/(X_n)$ and $A_{n-1} = F_{2^d}[X]/(X_{n-1})$, we have the following lemma:

Lemma 3.4.2 *Let φ the map defined by:*

$$\begin{array}{rcl} \varphi & : & A_{n-1} \to A_n \\ P + (X_{n-1}) & \to & P + (X_n) \end{array}$$

where $P \in F_{2^d}[X]$, then φ is an injective homomorphism of rings.

Proof. φ is clearly an homomorphism of rings.Let $P + (X_{n-1}) \in \ker \varphi$. Then,
$\varphi(P + (X_{n-1})) = 0 + (X_n)$ and $P + (X_n) = 0 + (X_n)$.
So, $P \in (X_n)$; and since $(X_n) \subseteq (X_{n-1})$ then, $P \in (X_{n-1})$. Thereby, φ is injective. ■

Remark 3.4.4 *A_{n-1}may be identified to $\varphi(A_{n-1})$, thereby A_{n-1}can be regarded as a subring of A_n.*

Conclusion

In this work, we present some notes on the The ring $\mathbb{F}_q[\varepsilon]$. Also we study their properties in specific cases.

Bibliography

[1] Boulbot, A., Chillali, A., & Mouhib, A. (2020). Elliptic curves over the ring R. Boletim da Sociedade Paranaense de Matemática, 38(3), 193-201.

[2] Chillali, A. (2011). Cryptography over elliptic curve of the ring. World Academy of Science, Engineering and Technology, 78, 848-850.

[3] Boulbot, A., Chillali, A., & Mouhib, A. (2016). Elliptic curves over the ring F_q [e], e^3= e^2. Gulf Journal of Mathematics, 4(4).

[4] Schaub, D. (1997). Eléments de la théorie des groupes. Licence de Mathématiques Univer (sité drAngers, 1997/1998.

[5] Virat, M. (2009). Courbes elliptiques sur un anneau et applications cryptographiques (Doctoral dissertation, Université Nice Sophia Antipolis).

[6] Demazure, M. (1997). Cours d'algèbre: primalité, divisibilité, codes (Vol. 1). Paris: Cassini.

[7] Ghadbane, N. (2020). Decomposition of groups and the wreath product of permutation groups. Applied Sciences, 22, 83-93.

[8] Ghadbane, N. (2019). The inverse monoid associated to a group and the semidirect product of groups. Journal of Algebra and Related Topics, 7(1), 25-34.

[9] McIvor, J. (2014). Ring Theory (Math 113), Summer 2014. University of California, Berkeley.

ملخص:

في هذه المذكرة، سوف ندرس العمليات الحسابية في حلقة حاصل القسمة $F_q[x]$ بواسطة كثير الحدود x^n ، $x^{n+1} = x^n$ ، $n = 1،2،3$ حيث F_q هو حقل منته عدد عناصره q.

سوف نتذكر بعض المعلومات والمفاهيم الأساسية حول الحلقات، كما سنقدم بعض الملاحظات حول العمليات الحسابية في الحلقات $F_q[e]$.

كلمات مفتاحية: المجموعة ،الحلقة ، الحقل ، المثالية ، المثالية القصوى ، حلقة حاصل القسمة ، تماثل الحلقات.

Abstract :

In this memory, we will study the arithmetic operations in the quotient ring of $F_q[x]$ by the polynomial x^n, $x^{n+1}=x^n$, n=1,2,3 where F_q is a finite field of order q.

We will recall some basic concepts about the rings. In addition, we will present some notes over the arithmetic operations in the Ring $F_q[e]$.

Keywords: Group, subgroup, ring, field, ideal, maximal ideal, quotient ring, Homomorphism Ring.

Résumé :

Dans ce mémoire, nous allons étudier les opérations arithmétiques dans l'anneau quotient de $F_q[x]$ par le polynôme x^n, $x^{n+1}=x^n$, n=1,2,3 où F_q est un corps fini d'ordre q.

Nous rappellerons quelques concepts de base sur les anneaux, nous présenterons également quelques notes sur les opérations arithmétiques dans l' anneau $F_q[e]$.

Most clés: Groupe, sous-groupe, anneau, corp, idéal, idéal maximal, anneau quotient, Homomorphism d'anneaux.