Background on

Groups, Rings, and Finite Fields

Andreas Klappenecker

September 12, 2002

A thorough understanding of the Agrawal, Kayal, and Saxena primality test requires some tools from algebra and elementary number theory. We collect here some basic definitions and facts. These notes cannot replace a standard text on algebra, but will hopefully provide enough background to make the beautiful result [1] accessible to a computer scientist. We provide numerous exercises so that the interested reader can gain a working knowledge in a short amount of time.

Groups. A **group** is a set G which is equipped with a binary operation $\circ\colon G \times G \to G$, such that

i) the associative law $(a \circ b) \circ c = a \circ (b \circ c)$ holds for all $a, b, c \in G$,
ii) there exists an identity $e \in G$ satisfying $a \circ e = e \circ a = a$ for all $a \in G$,
iii) each element $a \in G$ has an inverse a^{-1} satisfying $a^{-1} \circ a = a \circ a^{-1} = e$.

The prototype example of a group G is given by a set of invertible $n \times n$ matrices with complex entries, such that G contains the identity matrix, is closed under matrix multiplication and matrix inversion. The composition $\circ$ is given by matrix multiplication, e is the identity matrix, and a^{-1} is the inverse matrix of a.

The example illustrates that the group operation $\circ$ is not necessarily commutative, that is, in general $a \circ b$ will not be the same as $b \circ a$. A group is called **abelian** if $a \circ b = b \circ a$ holds for all $a, b \in G$. The number of elements in G is called the **order** of G. A group of finite order is said to be **finite**.

X1 Construct a *finite* non-abelian group.

An example of an abelian group is given by the set of integers $\mathbf{Z}$ with $\circ$ given by addition. Another example is given by the finite set $\mathbf{Z}/n\mathbf{Z} =$

$\{0, 1, \cdots, n-1\}$, where $n > 1$ is an integer and $\circ$ denotes addition of integers modulo n. The nonzero complex numbers $\mathbf{C}^*$ with $\circ$ given by multiplication is also an abelian group.

X2 Is the set of non-negative integers $\mathbf{Z}_{\geq 0}$ with the usual addition a group?

Let $(G, \circ)$ be a group. A nonempty subset H of G such that $x \circ y \in H$ and $x^{-1} \in H$ for all $x, y \in H$ is called a **subgroup** of G. The subgroup H is apparently a group. The notation $H \leq G$ means that H is a subgroup of G. The set $g \circ H = \{g \circ h \mid h \in H\}$, $g \in G$, is called a **left coset** of H in G.

For example, the set $G = \mathbf{Z}/4\mathbf{Z} = \{0, 1, 2, 3\}$ with addition modulo 4 is a group (with composition $\circ$ written as addition). The subset $H = \{0, 2\}$ is a subgroup of G. The set $1 + H = \{1, 3\}$ is a coset of H in G. Notice that $0 + H = 2 + H$ and that $1 + H = 3 + H$.

X3 Let G be a group, $H \leq G$. Show that $|H| = |g \circ H|$ for all $g \in G$. Show that either $m \circ H = n \circ H$ or $m \circ H \cap n \circ H = \emptyset$ holds for $m, n \in G$.

X4 Let G be a finite group, $H \leq G$. Prove that $|H|$ divides $|G|$.

We abbreviate the composition $a \circ a \circ \cdots \circ a$ of n times of a by a^n. We write a^{-n} for the inverse of a^n. It is understood that $a^0 = e$. The group operation $\circ$ is sometimes written additively $a \circ b = a + b$. The identity element is then denoted by 0, the inverse of an element a by $-a$, and a^n is expressed by na.

Let X be a subset of a group G. Then $\langle X \rangle$ denotes the smallest subgroup of G containing X, called the **subgroup of G generated by X**. Notice that

$$\langle X \rangle = \{g_1^{a_1} \cdots g_\ell^{a_\ell} \mid g_i \in X, a_i \in \mathbf{Z}, \ell \in \mathbf{Z}, \ell \geq 1\}.$$

A group G is called **cyclic** if and only if there exists an element $a \in G$ such that $G = \langle a \rangle$. For instance, the additive group of integers $\mathbf{Z}$ is a cyclic group generated by the element 1. Similarly, $\mathbf{Z}/n\mathbf{Z}$ with addition modulo n is a cyclic group generated by 1.

X5 Is the set $\mathbf{Z} \times \mathbf{Z}$ with the usual composition $(a, b) + (c, d) = (a + c, b + d)$ a cyclic group?

Let G be a finite group. The **order** of an element $g \in G$ is defined to be the smallest exponent such that $g^k = 1$. The set $\{1, g, g^2, \cdots, g^{k-1}\}$ coincides with the cyclic group $\langle g \rangle$ generated by g. It follows from X4 that the order of g must divide $|G|$. In particular, we have $g^{|G|} = 1$ for all elements $g \in G$.

X6 Prove Fermat's Little Theorem: If p is a prime, and $\gcd(a,p) = 1$, then $a^{p-1} \equiv 1 \bmod p$.

If p is a prime, then the subset $(\mathbf{Z}/p\mathbf{Z})^*$ of nonzero elements of $\mathbf{Z}/p\mathbf{Z}$ forms a group under multiplication modulo p. Gauß proved that $(\mathbf{Z}/p\mathbf{Z})^*$ is a cyclic group. For instance, if $p = 5$, then $(\mathbf{Z}/p\mathbf{Z})^* = \{1, 2, 3, 4\}$ is generated by 2, since $\langle 2 \rangle = \{2^0, 2^1, 2^2, 2^3\} = \{1, 2, 4, 3\}$.

Rings and Fields. A **ring** is a set R which is equipped with two binary operations, called addition and multiplication, such that

i) R is an abelian group under addition,
ii) multiplication is associative and posseses an identity element,
iii) multiplication is distributive with respect to addition.

We denote addition by $a + b$, and multiplication by juxtaposition ab. The identity element of addition is denoted by 0, and 1 denotes the identity element for multiplication. The ring R is said to be **commutative** if multiplication is commutative. A **field** is a commutative ring with $1 \neq 0$ in which every nonzero element is invertible with respect to multiplication.

X7 Explicitly state the axioms of a ring, a commutative ring, a field.

X8 Determine whether the set of 2×2 matrices over the real numbers with matrix addition and matrix multiplication as binary operations is a ring, a commutative ring, a field.

The set $\mathbf{Z}$ of integers with the usual addition and multiplication is an example of a commutative ring. The set $\mathbf{Z}/n\mathbf{Z} = \{0, 1, \ldots, n-1\}$ with addition modulo n and multiplication modulo n is another example of a commutative ring.

X9 Show that $ab = ac$, $a \neq 0$, does not necessarily imply $b = c$ in a ring. Does this law hold in a field?

X10 Show that $\mathbf{Z}/n\mathbf{Z}$ is a field if and only if n is a prime.

Polynomial Rings. A polynomial over a commutative ring R is an expression of the form

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$

where the coefficients a_i, $0 \leq i \leq n$, are elements of R and x is a variable with indeterminate meaning. The set of all such expressions is denoted by $R[x]$. The polynomial $0x^{m+n} + \cdots + 0x^{n+1} + a_n x^n + \cdots + a_1 x + a_0$ is regarded as the same polynomial as $f(x)$. If $a_n \neq 0$, then n is called the degree of $f(x)$, denoted by $\deg f(x)$. In this case $a_n = \mathrm{lc}(f(x))$ is called the leading coefficient of $f(x)$.

Let $g(x) = b_m x^m + \cdots + b_1 x + b_0$ be a polynomial in $R[x]$. Addition of polynomials is defined by

$$f(x)+g(x) = b_m x^m + \cdots + b_{n+1}x^{n+1} + (a_n+b_n)x^n + \cdots + (a_1+b_1)x + (a_0+b_0),$$

where we assumed without loss of generality that $m \geq n$. The multiplication of polynomials is defined by

$$f(x)g(x) = c_{m+n}x^{m+n} + \cdots + c_2x^2 + c_1x + c_0, \text{ where } c_k = \sum_{i+j=k} a_i b_j.$$

X11 Let R be a commutative ring. Show that $R[x]$ is a commutative ring.

Let p be a prime. We denote by $\mathbf{F}_p$ the finite field $\mathbf{Z}/p\mathbf{Z}$. The ring $\mathbf{F}_p[x]$ has a Euclidean division with remainder. The consequence is that this ring resembles in many ways the ring of integers.

X12 Let $f, g \in \mathbf{F}_p[x]$ with $g \neq 0$. Prove that there exist elements $q, r \in \mathbf{F}_p[x]$ such that $f(x) = q(x)g(x) + r(x)$, where $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Ideals. An **ideal** in a commutative ring R is an additive subgroup I of R such that if $r \in R$ and $s \in I$, then $rs \in I$. An ideal I is said to be generated by a subset $S \subset I$ if and only if each element $t \in I$ can be written in the form $t = \sum_{i=1}^{n} r_i s_i$ for some $r_i \in R$ and $s_i \in I$. We denote the ideal generated by the subset $S \subset R$ by $\langle S \rangle$. An ideal is said to be **principal** if and only if it can be generated by a single element in R.

For example, in the ring $\mathbf{Z}$ of integers, the ideal $\langle 6, 15 \rangle$ is given by the set $\langle 6, 15 \rangle = \{6n + 15m \mid n, m \in \mathbf{Z}\} = \{3m \mid m \in \mathbf{Z}\}$.

X13 Prove that every ideal in $\mathbf{F}_p[x]$ is a principal ideal.

X14 Prove: if $\langle d(x) \rangle = \langle a(x), b(x) \rangle$ in $\mathbf{F}_p[x]$, then $d(x) = \gcd(a(x), b(x))$.

Let I be an ideal of a commutative ring R. The cosets $r+I$, $r \in R$, form a partition of R, because I is in particular a subgroup of the additive group of R. Two elements $a, b \in R$ are called **congruent modulo** I if and only if they belong to the same coset of I. We denote the congruence of a and b by

$$a \equiv b \mod I.$$

In other words, $a \equiv b \bmod I$ if and only if $a - b \in I$.

X15 Explain the meaning of $a(x) \equiv b(x) \bmod \langle n, x^r - 1\rangle$ in $\mathbf{Z}[x]$.

X16 If $a \equiv b \bmod I$ and $c \equiv d \bmod I$, then $a+c \equiv b+d \bmod I$ and $ac \equiv bd \bmod I$.

An ideal I of a commutative ring R allows to define a new ring, the **residue class ring** R/I. The elements of R/I are the cosets $r+I$ of the ideal I. The addition and multiplication operations are respectively defined by

$$(a+I)+(b+I) = (a+b)+I, \quad (a+I)(b+I) = ab+I.$$

The axioms of a commutative ring are easily verified for R/I.

The prototype example is the ring $\mathbf{Z}$ of integers. An ideal in $\mathbf{Z}$ is of the form $n\mathbf{Z}$, since all ideals are principal in $\mathbf{Z}$. The residue class ring $\mathbf{Z}/n\mathbf{Z}$ gives then the usual modular arithmetic.

Finite Fields. Fields with a finite number of elements find applications in algorithms of cryptography or coding theory, and in numerous number theoretic algorithms. We begin by looking at a few small fields.

The arithmetic of the field $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$ with two elements can be summarized by

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Similarly, the arithmetic of the finite field $\mathbf{F}_3 = \mathbf{Z}/3\mathbf{Z}$ is fully described by

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

A finite field with four element exists. However, we have convinced ourselves in exercise X10 that is cannot be of the form $\mathbf{Z}/4\mathbf{Z}$. The idea is to construct this field as a residue class ring of $\mathbf{F}_2[x]$ modulo an ideal I.

We already know that $F = \mathbf{F}_2[x]/I$ is a commutative ring. We need to choose the ideal I such that each element $r + I \neq 0 + I$ of F is invertible, which means that there exists a residue class $s+I$ such that $(r+I)(s+I) = rs + I = 1 + I$.

Recall that an ideal in $\mathbf{F}_p[x]$ is of the form $\langle h(x) \rangle$ by X13. A nonconstant polynomial in $\mathbf{F}_p[x]$ is said to be irreducible if it cannot be written as a product of polynomials of postivie degree.

X17 Let p be a prime, $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, $h(x) \in \mathbf{F}_p[x]$ with $\deg h(x) > 1$. Show that the residue class ring $\mathbf{F}_p[x]/\langle h(x) \rangle$ is a field if and only if $h(x)$ is an irreducible polynomial in $\mathbf{F}_p[x]$.

The construction of a finite field with four elements in now a simple matter. Note that the polynomial $h(x) = x^2 + x + 1$ is irreducible in $\mathbf{F}_2[x]$. The residue classes of $\mathbf{F}_2[x]/\langle x^2 + x + 1 \rangle$ are given by the four elements

$$0 + \langle x^2 + x + 1 \rangle,\ 1 + \langle x^2 + x + 1 \rangle,\ x + \langle x^2 + x + 1 \rangle,\ 1 + x + \langle x^2 + x + 1 \rangle.$$

For simplicity, we will calculate with the representatives $0, 1, x, 1+x$ modulo the polynomial $x^2 + x + 1$ in $\mathbf{F}_2[x]$. The addition of the elements x and $x+1$ yields 1 in $\mathbf{F}_2[x]$. The multiplication of x and $x+1$ yields $x(x+1) = x^2 + x$ which is equivalent to 1 modulo $x^2 + x + 1$. Proceeding in this way, we can summarize the arithmetic rules of the field $\mathbf{F}_4 \cong \mathbf{F}_2[x]/\langle x^2 + x + 1 \rangle$ by

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

$\cdot$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

X18 Construct a finite field $\mathbf{F}_8$ with 8 elements.

A finite field F has always a subfield with a prime number of elements. This subfield $\mathbf{F}_p$ is obtained by repeatedly adding the identity 1 of F to itself. The field F can be interpreted as a vector space over $\mathbf{F}_p$. It follows the number of elements of a finite field is a prime power. If $\dim_{\mathbf{F}_p} F = n$, then F contains p^n elements.

It can be shown that there exist irreducible polynomials in $\mathbf{F}_p[x]$ of any given degree n. It turns out that any two fields with p^n elements are isomorphic. Therefore, any finite field can be obtained by the residue class ring construction $\mathbf{F}_p[x]/\langle h(x)\rangle$, which we have described above.

It should be noted that the multiplicative group of nonzero elements of a finite field is always a cyclic group. For example, there exists a polynomial $g(x) \in \mathbf{F}_p[x]$ such that any nonzero element $f(x) + \langle h(x)\rangle$ in the finite field $\mathbf{F}_p[x]/\langle h(x)\rangle$ is of the form $g(x)^m + \langle h(x)\rangle$ for some integer m.

Final Remarks. There is of course much more that can be said about finite fields, rings, and groups. For a computer scientist, however, I would recommend to toy around with the ideas presented here. A computer algebra system is the perfect companion for further explorations. Good choices are GAP, MAGMA, Mathematica, or Maple.

References

[1] M. Agrawal, N. Kayal, and N. Saxena. Primes is in P. Preprint, IIT Kanpur, August 2002.

[2] N. Jacobson. *Basic Algebra I.* W.H. Freeman and Company, New York, 2nd edition, 1985.

Acknowledgments. Many thanks to Professor Jianer Chen, Avanti Ketkar, and Santosh Kumar for corrections and helpful comments.

Solutions

S1 Let G be the set of invertible 2×2 matrices over the field with two elements $\mathbf{F}_2 = \{0, 1\}$. The group contains six elements, and is non-abelian, since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

S2 No, since there is no integer $a \geq 0$ such that $1 + a = 0$.

S3 Notice that $x \mapsto g \circ x$ is a bijective mapping, thus $|H| = |g \circ H|$. To prove the second statement, notice that there is nothing to prove if $m \circ H$ and $n \circ H$ are disjoint. Thus, let $k \in m \circ H$ and $k \in n \circ H$. Thus, there exist $h_1, h_2 \in H$ such that $k = m \circ h_1 = n \circ h_2$. Hence $m \circ h_1 \circ h_2^{-1} = n$, and $m \circ h_1 \circ h_2^{-1} \circ h = n \circ h$ for all $h \in H$. Thus, $n \circ H \subseteq m \circ H$. Similarly, $m \circ H \subseteq n \circ H$.

S4 By exercise X3, G is partitioned by the cosets of H, and all have the same size $|H|$. Thus $|G|$ is a multiple of $|H|$.

S5 No. If $\mathbf{Z} \times \mathbf{Z}$ were generated by a single element (a, b), then all elements would be of the form (na, nb) for some $n \in \mathbf{Z}$. It immediately follows that a and b have to equal 1, since the projection onto one coordinate must be $\mathbf{Z}$. This would imply that the cyclic group just generates the diagonal of $\mathbf{Z} \times \mathbf{Z}$, contradiction.

S6 We can regard a as an element of $(\mathbf{Z}/p\mathbf{Z})^*$. Note that $\gcd(a, p) = 1$ and $\gcd(b, p) = 1$ implies $\gcd(ab, p) = 1$. We also have $\gcd(1, p) = 1$. Since $\gcd(a, p) = 1 = ar + ps$, we have that $a^{-1} = r$ is a nonzero element in $\mathbf{Z}/p\mathbf{Z}$. Therefore, $(\mathbf{Z}/p\mathbf{Z})^*$ is a group, since it contains the identity 1, is closed under multiplication, and contains an inverse for each element. The order of this group is $p - 1$, hence $a^{p-1} = 1$ in $(\mathbf{Z}/p\mathbf{Z})^*$. This proves the claim.

S7 We can express the axioms of a ring by the following identities:

$$
\begin{aligned}
a + (b + c) &= (a + b) + c && \text{(associativity of addition)} \\
0 + a &= a + 0 && \text{(zero is the identity of addition)} \\
(-a) + a &= a + (-a) = 0 && \text{(negative)} \\
a + b &= b + a && \text{(commutativity of addition)} \\
a\,(b\,c) &= (a\,b)\,c && \text{(associativity of multiplication)} \\
a\,1 &= 1\,a = a && \text{(unit element)} \\
(a + b)c &= ac + bc && \text{(left distributive law)} \\
a(b + c) &= ab + ac && \text{(right distributive law)}
\end{aligned}
$$

A commutative ring also satisfies $ab = ba$. A field is a commutative ring that satisfies $1 \neq 0$ as well as $a^{-1}a = aa^{-1} = 1$ for all $a \neq 0$.

S8 The multiplication of matrices is not commutative, thus the set it is not a commutative ring, in particular not a field. The usual rules for matrix addition and multiplication imply that the set is a ring.

S9 Let $\mathbf{Z}/4\mathbf{Z}$. Then $2 \cdot 2 = 2 \cdot 0 = 0$, but $2 \neq 0$. In a field, the element a has an inverse a^{-1}, implying $b = a^{-1}(ab) = a^{-1}(bc) = c$.

S10 If $n = 1$, then $1 = 0$ in $\mathbf{Z}/n\mathbf{Z}$, hence it is not a field. We may assume that $n > 1$. Suppose that n is composite, $n = ab$ with $a, b \neq 1$. Then $ab = a0$ but $b \neq 0$, because $n > 1$. Since this cancellation law does not hold, $\mathbf{Z}/n\mathbf{Z}$ cannot be a field by exercise X9. If p is a prime, then $\mathbf{Z}/p\mathbf{Z}$ is a commutative ring in which $1 \neq 0$ and every element $a \neq 0$ has a multiplicative inverse (which can be found using the extended Euclidean algorithm), hence $\mathbf{Z}/p\mathbf{Z}$ is a field.

S11 Routine verification, see Section 2.10 in [2].

S12 Let $n = \deg f(x)$, $m = \deg g(x)$, and $\alpha = \mathrm{lc}(f(x))$, $\beta = \mathrm{lc}(g(x))$. We prove the result by induction on n. If $n < m$, then $q(x) = 0$ and $r(x) = f(x)$ does the job. If $n \geq m$, then the polynomial $f_0(x) = f(x) - \alpha\beta^{-1}x^{n-m}g(x)$ has degree smaller than $f(x)$. By induction, there exist polynomials $q_0(x), r_0(x)$ such that $f_0(x) = q_0(x)g(x) + r_0(x)$ with $r_0(x) = 0$ or $\deg r_0(x) < \deg g(x)$. Let $q(x) = \alpha\beta^{-1}x^{n-m} + q_0(x)$ and $r(x) = r_0(x)$. This choice gives $f(x) = q(x)g(x) + r(x)$, as desired.

S13 Let I be a ideal in $\mathbf{F}_p[x]$. If $I = \langle 0 \rangle$, then we are done. If not, then I must contain a nonzero element. Choose an element $s(x) \neq 0$ of I of minimal degree. If $t(x)$ is an arbitrary element of I, then $t(x) = q(x)s(x) + r(x)$ with $r(x) = 0$ or $\deg r(x) < \deg s(x)$. Suppose that $r(x) \neq 0$, which means that $\deg r(x) < \deg s(x)$. Since $s(x), t(x) \in I$, we have $r(x) = t(x) - q(x)s(x) \in I$. However, $r(x)$ is of smaller degree than $s(x)$, contradiction. Therefore, $r(x) = 0$, and we can conclude that all elements in the ideal I are multiples of $s(x)$, that is, $I = \langle s(x) \rangle$.

S14 We have $a(x) = g(x)d(x)$ and $b(x) = h(x)d(x)$, since $\langle a(x), b(x) \subseteq \langle d(x) \rangle$. Hence $d(x)$ is a common divisor of $a(x)$ and $b(x)$. Since $\langle d(x) \rangle \subseteq \langle a(x), b(x) \rangle$, we have $d(x) = a(x)r(s) + b(x)s(x)$ for some $r(x), s(x) \in \mathbf{F}_p[x]$. Thus, any common divisor of $a(x)$ and $b(x)$ must divide $d(x)$.

S15 The notation means that there exist polynomials $g(x), h(x) \in \mathbf{Z}[x]$ such that $a(x) - b(x) = ng(x) + (x^r - 1)h(x)$, that is, $a(x) = b(x) + ng(x) + (x^r - 1)h(x)$.

S16 By assumption, $a - b$ and $c - d$ are elements of I. Thus $(a - b) + (c - d) = (a + c) - (b + d) \in I$, which shows that $a + c \equiv b + d \bmod I$. Moreover, $(a - b)c$ and

$b(c-d)$ are elements of I, hence $(a-b)c+b(c-d)=ac-bd\in I$, which proves $ac\equiv bd \bmod I$.

S17 The nonzero elements of $\mathbf{F}_p[x]/\langle h(x)\rangle$ can be assumed to be of the form $g(x)+\langle h(x)\rangle$ with $g(x)\neq 0$ and $\deg g(x)<\deg h(x)$. If $h(x)$ is irreducible, then $\gcd(g(x),h(x))=1=g(x)r(x)+h(x)s(x)$ for some polynomials $r(x),s(x)\in\mathbf{F}_p[x]$ by exercise X13. Hence, $r(x)$ is the inverse of $g(x)$ modulo $h(x)$. It follows that $\mathbf{F}_p[x]/\langle h(x)\rangle$ is a finite field provided that $h(x)$ is irreducible. On the other hand, if $h(x)$ is reducible, then there exist polynomials $f(x),g(x)\in\mathbf{F}_p[x]$ of degree >1 such that $h(x)=f(x)g(x)$. Note that $g(x)0=g(x)f(x)$ in $\mathbf{F}_p[x]/\langle h(x)\rangle$ does not imply $f(x)=0$, hence the cancellation law does not hold, whence $\mathbf{F}_p[x]/\langle h(x)\rangle$ cannot be a field by exercise X9.

S18 The polynomial $h(x)=x^3+x^2+1$ is irreducible in $\mathbf{F}_2[x]$. The field is given by $\mathbf{F}_2[x]/\langle h(x)\rangle$. We leave the construction of addition and multiplication table to the reader.