CHAPTER 4

Mathematics of Cryptography Part II: Algebraic Structures

(Solution to Odd-Numbered Problems)

Review Questions

1. The combination of the set and the operations that are applied to the elements of the set is called an *algebraic structure*. We have defined three common algebraic structures: *groups*, *rings*, and *fields*.

3. A ring is an algebraic structure with two operations. The first operation must satisfy all five properties required for an abelian group. The second operation must satisfy only the first two. In addition, the second operation must be distributed over the first. A commutative ring is a ring in which the commutative property is also satisfied for the second the operation.

5. A Galois field, GF(p^n), is a finite field with p^n elements. If $n = 1$, the field is sometimes referred to as GF(p).

7. An example of a ring is $\mathbf{R} = <\mathbf{Z}, +, \times>$. For the first operation, the identity element is 0; the inverse of an element a is $-a$. Neither the identify element nor the inverse of an element is defined for the second operation.

9. A polynomial of degree $n - 1$ with coefficient in GF(2) can represent an n-bit word with power of each term defining the position of the bit and the coefficients of the terms defining the value of the bits.

Exercises

11. The group $\mathbf{G} = <\mathbf{Z}_4, +>$ has only four members: 0, 1, 2, and 3.

a. For all a's and b's members of G, we need to prove that $a + b = b + a$. The following shows the proof (all operations are modulo 4).

$$(0 + 1) = (1 + 0) \qquad (0 + 2) = (2 + 0) \qquad (0 + 3) = (3 + 0)$$
$$(1 + 2) = (2 + 1) \qquad (1 + 3) = (3 + 1)$$
$$(2 + 3) = (3 + 2)$$

b.

$$(3 + 2) \bmod 4 = 1 \bmod 4 \qquad (3 - 2) \bmod 4 = -1 \bmod 4 = 3 \bmod 4$$

13. Assume that the operation is ($\blacklozenge$). We can say that ($x \blacklozenge y$) is the same as $x \bullet (-y)$, in which ($-y$) is the inverse of y with respect to operation ($\bullet$). Using Table 4.1, we can create the following table:

$\blacklozenge$	*a*	*b*	*c*	*d*
a	*a*	*d*	*c*	*b*
b	*b*	*a*	*d*	*c*
c	*c*	*b*	*a*	*d*
d	*d*	*c*	*b*	*a*

Another way to solve the problem is to think about similarity between the group represented in Table 4.1 and the group $\mathbf{G} = \langle \mathbf{Z}_4, + \rangle$. Make the table for subtraction operation in the group $\mathbf{G} = \langle \mathbf{Z}_4, + \rangle$ and replace 0 with *a*, 1 with *b*, 2 with *c*, and 3 with *d*.

15. We use only two cases:

a. We first prove that

$$\mathbf{([1\ 3\ 2] \circ [2\ 1\ 3]) \circ [3\ 1\ 2] = [1\ 3\ 2] \circ ([2\ 1\ 3] \circ [3\ 1\ 2])}$$

$$\mathbf{([1\ 3\ 2] \circ [2\ 1\ 3]) \circ [3\ 1\ 2] = [3\ 1\ 2] \circ [3\ 1\ 2] = [2\ 3\ 1]}$$
$$\mathbf{[1\ 3\ 2] \circ ([2\ 1\ 3] \circ [3\ 1\ 2]) = [1\ 3\ 2] \circ [3\ 2\ 1] = [2\ 3\ 1]}$$

b. We then prove that

$$\mathbf{([1\ 2\ 3] \circ [2\ 1\ 3]) \circ [3\ 1\ 2] = [1\ 2\ 3] \circ ([2\ 1\ 3] \circ [3\ 1\ 2])}$$

$$\mathbf{([1\ 2\ 3] \circ [2\ 1\ 3]) \circ [3\ 1\ 2] = [2\ 1\ 3] \circ [3\ 1\ 2] = [3\ 2\ 1]}$$
$$\mathbf{[1\ 2\ 3] \circ ([2\ 1\ 3] \circ [3\ 1\ 2]) = [1\ 2\ 3] \circ [3\ 2\ 1] = [3\ 2\ 1]}$$

17. The result of ([1 3 2] $\circ$ [3 2 1]) $\circ$ [2 1 3] = **[3 2 1]**. Bob can use the permutation [3 2 1] to reverse the operation. This proves that double or multiple permutation does not help; Alice could have used one single permutation.

19.

a. The order of the group is $|\mathbf{G}| = 18$. The order of potential subgroups should divide 18, which means $|\mathbf{H}|$ can be 1, 2, 3, 6, 9, and 18.

b. The order of the group is $|\mathbf{G}| = 29$. The order of potential subgroups should divide 29, which means $|\mathbf{H}|$ can be 1 and 29.

c. The order of the group is $|\mathbf{G}| = 4$. The order of potential subgroups should divide 4, which means $|\mathbf{H}|$ can be 1, 2, and 4.

d. The order of the group is $|\mathbf{G}| = 18$. The order of potential subgroups should divide 18, which means $|\mathbf{H}|$ can be 1, 2, 3, 6, 9, and 18.

21. The elements 0, g^0, g^1, g^2, and g^3 can be easily be generated, because they are the 4-bit representations of 0, 1, x^2, and x^3. We use the relation $f(g) = g^4 + g^3 + 1 = 0$ to generate other powers. Using this relation, we have $g^4 = g^3 + 1$. We use this relation to find the value of all elements as 4-bit words:

$$
\begin{array}{lllll}
0 = 0 & = 0 & = 0 & \longrightarrow & 0 = (0000) \\
g^0 = g^0 & = g^0 & = g^0 & \longrightarrow & g^0 = (0001) \\
g^1 = g^1 & = g^1 & = g^1 & \longrightarrow & g^1 = (0010) \\
g^2 = g^2 & = g^2 & = g^2 & \longrightarrow & g^2 = (0100) \\
g^3 = g^3 & = g^3 & = g^3 & \longrightarrow & g^3 = (1000) \\
g^4 = g^4 & = g^4 & = g^3 + 1 & \longrightarrow & g^4 = (1001) \\
g^5 = g\,(g^4) & = g\,(g^3 + 1) & = g^3 + g + 1 & \longrightarrow & g^5 = (1011) \\
g^6 = g\,(g^5) & = g\,(g^3 + g + 1) & = g^3 + g^2 + g + 1 & \longrightarrow & g^6 = (1111) \\
g^7 = g\,(g^6) & = g\,(g^3 + g^2 + g + 1) & = g^2 + g + 1 & \longrightarrow & g^7 = (0111) \\
g^8 = g\,(g^7) & = g\,(g^2 + g + 1) & = g^3 + g^2 + g & \longrightarrow & g^8 = (1110) \\
g^9 = g\,(g^8) & = g\,(g^3 + g^2 + g) & = g^2 + 1 & \longrightarrow & g^9 = (0101) \\
g^{10} = g\,(g^9) & = g\,(g^2 + 1) & = g^3 + g & \longrightarrow & g^{10} = (1010) \\
g^{11} = g\,(g^{10}) & = g\,(g^3 + g) & = g^3 + g^2 + 1 & \longrightarrow & g^{11} = (1101) \\
g^{12} = g\,(g^{11}) & = g\,(g^3 + g^2 + 1) & = g + 1 & \longrightarrow & g^{12} = (0011) \\
g^{13} = g\,(g^{12}) & = g\,(g + 1) & = g^2 + g & \longrightarrow & g^{13} = (0110) \\
g^{14} = g\,(g^{13}) & = g\,(g^2 + g) & = g^3 + g^2 & \longrightarrow & g^{14} = (1100)
\end{array}
$$

23.

a. We show two examples of multiplication (using the results of Exercise 21):

$$
\begin{array}{lll}
g^3 \times g^{12} = g^{15 \bmod 15} = g^0 = 1 & \rightarrow & (0001) = (1000) \times (0011) \\
g^{10} \times g^{12} = g^{22 \bmod 15} = g^7 = g^2 + g + 1 & \rightarrow & (0111) = (1010) + (0011)
\end{array}
$$

b. We show two examples of division (using the results of Exercise 21):

$$
\begin{array}{lll}
g^3 \div g^9 = g^{-6 \bmod 15} = g^9 = g^2 + 1 & \rightarrow & (0101) = (1000) \div (0101) \\
g^{10} \div g^4 = g^{6 \bmod 15} = g^6 = g^3 + g^2 + g + 1 & \rightarrow & (1111) = (1010) - (1001)
\end{array}
$$

25.

a. $x^4 + x$

b. x

c. $x^5 + 1$

d. $x + 1$

27.

a. $5 + 3 = 8 \bmod 7 = 1 \bmod 7$

b. $5 - 4 = 1 \bmod 7$

c. $5 \times 3 = 15 \bmod 7 = 1 \bmod 7$

d. $5 \div 3 = 5 \times (3^{-1}) = 5 \times 5 = 25 \bmod 7 = 4 \bmod 7$

29. A polynomial $f(x)$ of degree n is irreducible if $f(x) = g(x) \times h(x)$, where g and h are two polynomials, each with the degree greater than zero. According to this definition we have **degree** (f) = **degree** (g) + **degree** (h). Based on this, a reducible polynomial of degree 2 can be factored only as two polynomials of degree 1 (2 = 1 + 1). In other words, a factors of a reducible polynomial of degree 2 can be only x or $(x + 1)$ (the only two polynomials of degree 1). We can check all polynomials of degree 2 to see which one can be factored as such.

$\mathbf{(x^2) = (x) \times (x)}$	$\rightarrow$	**(x^2) is reducible**
$\mathbf{(x^2 + 1) = (x + 1) \times (x + 1)}$	$\rightarrow$	**$(x^2 + 1)$ is reducible**
$\mathbf{(x^2 + x) = (x) \times (x + 1)}$	$\rightarrow$	**$(x^2 + x)$ is reducible**
$(x^2 + x + 1)$ cannot be factored.	$\rightarrow$	**$(x^2 + x + 1)$ is irreducible**

It can also be proved that $\boldsymbol{f(x) = x^2 + x + 1}$ cannot be evenly divided by x or $x + 1$ because this implies that $x = 0$ or $x = -1$ must be the root of the $f(x)$, which are not $(f(0) = 1$ and $f(-1) = 1)$.

31. We first write each number as a polynomial with coefficient in GF(2). We then multiply the polynomials. Finally, we convert the result to the binary pattern.

a. $(x + 1) \times (x + 1) \rightarrow (x^2 + x + x + 1) \rightarrow (x^2 + 1) \rightarrow 101$

b. $(x^3 + x) \times (x^3) \rightarrow (x^6 + x^4) \rightarrow 1010000$

c. $(x^4 + x^3 + x^2) \times (x^4) \rightarrow (x^{16} + x^7 + x^6) \rightarrow 10000000011000000$

33. The inverse is $\boldsymbol{x^3 + x}$, as shown below (using the extended Euclidean algorithm).

q	r_1	r_2	r	t_1	t_2	t
$x + 1$	$x^5 + x^2 + 1$	$x^4 + x^3 + 1$	$x^3 + x^2 + x$	0	1	$x + 1$
x	$x^4 + x^3 + 1$	$x^3 + x^2 + x$	$x^2 + 1$	1	$x + 1$	$x^2 + x + 1$
$x + 1$	$x^3 + x^2 + x$	$x^2 + 1$	1	$x + 1$	$x^2 + x + 1$	$x^3 + x$
$x^2 + 1$	$x^2 + 1$	1	0	$x^2 + x + 1$	$x^3 + x$	1
	1	0		$\boldsymbol{x^3 + x}$	1	

35. We use Table 4.10 to find the multiplicative inverse of the second word. We then use the same table to multiply the first word with the inverse of the second word.

a. $(100) \div (010) = (100) \times (010)^{-1} = (100) \times \mathbf{(110)} = (010)$

b. $(100) \div (000) \rightarrow$ This operation is impossible because (000) has no inverse.

c. $(101) \div (011) = (101) \times (011)^{-1} = (101) \times \mathbf{(100)} = (011)$

d. $(000) \div (111) = (000) \times (111)^{-1} = (000) \times \mathbf{(101)} = (111)$

37. We let $P_1 = (10000)$, $P_2 = (10101)$, and modulus = (100101). The following table shows the process:

Powers	*Shift-LetOperation*	*Exclusive-Or*
$x^0 \otimes P_2$		10101
$x^1 \otimes P_2$	01010	$01010 \oplus 00101 = 01111$
$x^2 \otimes P_2$	11110	11110
$x^3 \otimes P_2$	11100	$11100 \oplus 00101 = 11001$
$\mathbf{x^4 \otimes P_2}$	**10010**	$\mathbf{10010 \oplus 00101 = 10111}$
$\mathbf{P_1 \otimes P_2 = (x^4 \otimes P_2) = 10111}$		

The result is **(10111)** or $\mathbf{(x^4 + x^2 + x + 1)}$, which can be proved using multiplication and division by the modulus.