Chapter 4. GROUPS, RINGS AND FIELDS

These are basic notions of abstract algebra, which is widely used in cryptography.

A **group** G, sometimes denoted by $\{G, \bullet\}$, is a set of elements with a binary operation, denoted by $\bullet$, that associates to each ordered pair (a,b) of elements in G an element $(a \bullet b)$ in G, such that the following axioms are obeyed:

(A1) Closure: If a and b belong to G, then $a \bullet b$ is also in G

(A2) Associative: $a \bullet (b \bullet c) = (a \bullet b) \bullet c$ for all a,b,c in G

(A3) Identity element: There is an element e in G such that $a \bullet e = e \bullet a = a$ for all a in G

(A4) Inverse element: For each a in G there is an element a' in G such that $a \bullet a' = a' \bullet a = e$

Example: set S_N of permutations on the set {1,2,..,N} with operation $\bullet$ - composition of permutations is a group with e=(1,2,..,N). For N=3, (123) $\bullet$(321)=(321); (213) $\bullet$(132)=(312)

If a group has a finite number of elements, it is referred to as a **finite group**, and the **order** of the group is equal to the number of elements in the group. Otherwise, the group is **infinite group.**

A group is said to be **abelian** if it satisfies the following additional condition:

(A5) Commutative: $a \bullet b = b \bullet a$ for all a,b in G

The set of integers (positive, negative, and 0) under addition is an abelian group. The set of real numbers under multiplication is an abelian group.

The set S_N of permutations is not an abelian group.

When the group operation is addition, the identity element is 0; the inverse element of a
is –a; and the subtraction is defined as: a-b=a+(-b).

Exponentiation within a group is defined as repeated application of the group operation, so that $a^3 = a \bullet a \bullet a$. We define also $a^0 = e$, the **identity element**, and $a^{-n} = (a')^n$, where a' is **inverse element** for a. A **group G is cyclic** if every element of G is a power a^k (k – integer) of a fixed element $a \in G$. The element a is said to **generate** the group G, or to be a **generator** of G. A cyclic group is always abelian, and may be finite or infinite.

GROUPS, RINGS AND FIELDS (CONT 1)

A **ring** R, sometimes denoted by {R,+,×}, is a set of elements with two binary operations, called addition and multiplication, such that for all a, b, c in R the following axioms are obeyed:

(A1-A5) R is an abelian group with respect to addition; that is, R satisfies axioms A1 through A5, For this case of an additive group we denote the identity element as 0 and the inverse of a as –a.

(M1) Closure under multiplication: If a and b belong to R, then ab is also in R (multiplication, as usually, is shown by concatenation of its operands)

(M2) Associativity of multiplication: a(bc)=(ab)c

(M3) Distributive laws: a(b+c)=ab+ac
(a+b)c=ac+bc

With respect to addition and multiplication, the set of all n-square matrices over the real numbers is a ring R.

The ring is said to be commutative if it satisfies the following additional condition:

(M4) Commutativity of multiplication: ab=ba

Let S be the set of all even integers under the usual operations of addition and multiplication. S is a commutative ring. The set of all n-square matrices over the real numbers is not a commutative ring.

We define integral domain, which is commutative ring that obeys the following axioms:

(M5) Multiplicative identity: There is an element 1 such that a1=1a=a for all a in R

(M6) No zero divisors: If a,b in R and ab=0, then, either a=0 or b=0.

Let S be the set of integers, positive, negative, and 0, under the usual operations of addition and multiplication. S is an integral domain.

A field F, sometimes denoted by {F,+,×}, is a set of elements with two operations, called addition and multiplication, such that for all a, b, c in F the following axioms are obeyed:

(A1-M6) F is an integral domain; that is, F satisfies axioms A1 through A5 and M1 through M6.

(M7) Multiplicative inverse: For each a in F, except 0, there is an element a^{-1} **in F, such that** $aa^{-1} = a^{-1}a = 1$

In essence, a field is a set in which we can do addition, subtraction, multiplication and division without leaving the set. Division is defined as: $a/b = a(b^{-1})$

GROUPS, RINGS AND FIELDS (CONT 2)

Examples of fields are the rational numbers, real numbers, complex numbers. Set of all integers is not a field, because not every element of the set has a multiplicative inverse; in fact, only the elements 1 and -1 have multiplicative inverses in integers.

Fig. 4.1 summarises axioms that define groups, rings and fields

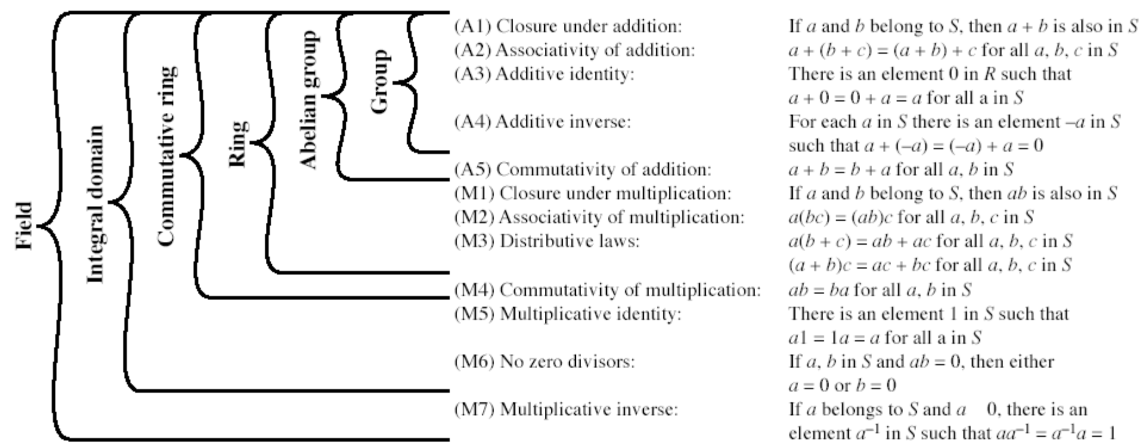

Figure 4.1 Group, Ring, and Field

MODULAR ARITHMETIC

Given any positive integer n and any integer a, if we divide a by n, we get an integer quotient q and an integer remainder r that obey the following relationship:

a=qn+r $0 \le r < n; q = \lfloor a/n \rfloor$

where $\lfloor x \rfloor$ is the largest integer less than or equal to x.

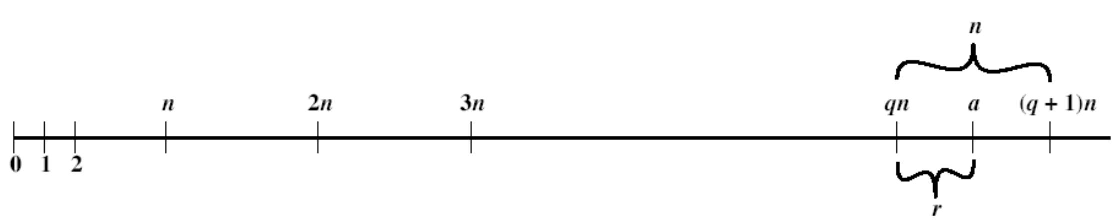

Figure 4.2 The Relationship $a = qn + r;\ 0 \le r < n$

The remainder r is often referred to as a residue.

MODULAR ARITHMETIC (CONT 1)

a=11, n=7, 11=1x7+4, r=4

a=-11, n=7, -11=(-2)x7+3, r=3

If a is an integer and n is a positive integer, we define a mod n to be the remainder when a is divided by n, Thus, for any integer a, we can always write

$a = \lfloor a/n \rfloor \times n + (a \bmod n)$

11mod7=4, -11mod7=3

Two integers a and b are said to be congruent modulo n, if a mod n = b mod n. This is written as $a \equiv b \bmod n$.

$73 \equiv 4 \bmod 23; 21 \equiv -9 \bmod 10$

Divisors

We say that a nonzero b divides a if a=mb for some m, where a, b, and m are integers. That is, b divides a if there is no remainder on division. The notation b|a is commonly used to mean b divides a. Also, if b|a, we say that b is a divisor of a.

The positive divisors of 24 are 1,2,3,4,6,8,12,24.

The following relations hold:

- If a|1 then a=$\pm$ 1
- If a|b and b|a, then a=$\pm$ b
- Any b$\neq$0 divides 0
- If b|g and b|h then b|(mg+nh) for arbitrary integers m and n

To see this last point, note that

If b|g, then g=b$\times$g1 for some integer g1

If b|h, then h=b$\times$h1 for some integer h1

So

mg+nh=mbg1+nbh1=b$\times$(mg1+nh1)

and therefore b divides mg+nh.

B=7,g=14, h=63, m=3, n=2

7|14 and 7|63. To show: 7|(3$\times$14+2$\times$63)

We have (3$\times$14+2$\times$63)=7(3$\times$2+2$\times$9)

And it is obvious that 7|7(3$\times$2+2$\times$9)

Note that if a$\equiv$0modn, then n|a.

Properties of the Modulo operator

1. a$\equiv$b mod n if n|(a-b)
2. a$\equiv$b mod n implies b$\equiv$a mod n
3. a$\equiv$b mod n and b$\equiv$c mod n imply a$\equiv$c mod n

Properties of the Modulo operator (CONT 1)

To demonstrate the 1st point, if n|(a-b), then a-b=kn for some k. So we can write a=b+kn. Therefore, (a mod n) (remainder when b+kn is divided by n) = (remainder when b is divided by n) = (b mod n)

$23 \equiv 8$ mod 5 because 23-8=15=5x3

$-11 \equiv 5$ mod 8 because -11-5=-16=8x(-2)

$81 \equiv 0$ mod 27 because 81-0=81=27x3

Modular arithmetic operations

Properties of modular arithmetic, working over {0,1,.., n-1}:

1. [(a mod n) + (b mod n)] mod n = (a+b) mod n
2. [(a mod n) - (b mod n)] mod n = (a-b) mod n
3. [(a mod n) x (b mod n)] mod n = (ab) mod n

We demonstrate the 1st property. Define (a mod n) = r_a and (b mod n) = r_b. Then we can write a=r_a+jn for some integer j and b= r_b+kn for some integer k. Then

(a+b) mod n = (r_a+jn+ r_b+kn) mod n = (r_a+ r_b+(k+j)n) mod n = (r_a+ r_b) mod n = [(a mod n) + (b mod n)] mod n

11 mod 8 =3, 15 mod 8 =7

[(11 mod 8) + (15 mod 8)] mod 8 = 10 mod 8 =2

(11+15) mod 8 = 26 mod 8 = 2

[(11 mod 8) - (15 mod 8)] mod 8 = -4 mod 8 =4

(11-15) mod 8 = -4 mod 8 = -4

[(11 mod 8) x (15 mod 8)] mod 8 = 21 mod 8 =5

(11x15) mod 8 = 165 mod 8 = 5

Exponentiation is performed, as in ordinary arithmetic

To find 11^7 mod 13, we can proceed as follows:

$$11^2 = 121 \equiv 4 \bmod 13$$

$$11^4 \equiv 4^2 \equiv 3 \bmod 13$$

$$11^7 \equiv 11 \times 4 \times 3 \equiv 132 \equiv 2 \bmod 13$$

Thus, the rules for ordinary arithmetic involving addition, subtraction, and multiplication carry over into modular arithmetic.

Modular arithmetic operations (CONT 1)

Table 4.1 Arithmetic Modulo 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

(a) Addition modulo 8

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

(c) Additive and multiplicative inverses modulo 8

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(b) Multiplication modulo 8

Table 4.1 introduces arithmetic modulo 8. We see that not for all elements exist multiplicative inverses (for 2, 4, 6).

Properties of modular arithmetic

Let Zn ={0,1,..,n-1}. This is referred to as the set of residues, or residue class modulo n. To be more precise, each integer in Zn represents a residue class. We can labe the residue classes modulo n as [0], [1],.., [n-1], where

[r]={a: a is integer, a$\equiv$r mod n}

Of all the integers in the residue class, the smallest nonnegative integer is the one usually used to represent the residue class. Finding the smallest nonnegative integer to which k is congruent modulo n is called reducing k modulo n.

Properties of modular arithmetic (CONT 1)

If we perform modulo arithmetic within Zn, the properties shown in Table 4.2 hold for integers in Zn. Thus, Zn is a commutative ring with a multiplicative identity element.

Table 4.2 Properties of Modular Arithmetic for Integers in Z_n

Property	Expression
Commutative laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive laws	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$ $[w + (x \times y)] \bmod n = [(w + x) \times (w + y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive inverse $(-w)$	For each $w \in Z_n$, there exists a z such that $w + z \equiv 0 \bmod n$

There is one peculiarity of modular arithmetic that sets it apart from ordinary arithmetic. First, observe that, as in ordinary arithmetic, we can write

If $(a+b) \equiv (a+c) \bmod n$ then $b \equiv c \bmod n$ (4.1)

$(5+23) \equiv (5+7) \bmod 8$, then $23 \equiv 7 \bmod 8$

Equation (4.1) is consistent with the existence of an additive inverse. Adding the additive inverse of a to both sided of (4.1), we have

$((-a)+a+b) \equiv ((-a)+a+c) \bmod n$

$b \equiv c \bmod n$

However, the following statement is true only with the attached condition:

If $(a \times b) \equiv (a \times c) \bmod n$ then $b \equiv c \bmod n$ if a is relatively prime to b (4.2)

Where the term relatively prime is defined as follows: Two integers are relatively prime if their only common positive integer factor is 1. Similar to the case of equation (4.1), we can say that (4.2) is consistent with the existence of a multiplicative inverse of a. Applying the multiplicative inverse of a to both sides of (4.2), we have

Properties of modular arithmetic (CONT 2)

$((a^{-1})ab) \equiv ((a^{-1})ac) \bmod n$

$b \equiv c \bmod n$

To see this, consider an example, in which condition does not hold:

6x3=18 $\equiv$ *2 mod 8*

6x7=42 $\equiv$ *2 mod 8*

Yet $3 \neq 7$ *mod 8 because 6 and 8 are not relatively prime*

With a=6 and n=8,

Z8	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
Multiply by 6:	*0*	*6*	*12*	*18*	*24*	*30*	*36*	*42*
Residues:	*0*	*6*	*4*	*2*	*0*	*6*	*4*	*2*

However, if we take a=5 and n=8, whose only common factor is 1,

Z8	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
Multiply by 5:	*0*	*5*	*10*	*15*	*20*	*25*	*30*	*35*
Residues:	*0*	*5*	*2*	*7*	*4*	*1*	*6*	*3*

The line of residues contains all integers in Z8, in a different order.

In general, an integer has a multiplicative inverse in Zn, if that integer is relatively prime to n. Table 4.1c shows that the integers 1, 3, 5, and 7 have a multiplicative inverse, but 2, 4, and 6 do not.

Euclud's algorithm

(3rd century B.C., from Alexandria)

One of the basic techniques of number theory is Euclid's algorithm, which is a simple procedure for determining the greatest common divisor of two positive numbers.

Greatest common divisor

We will use notation gcd(a,b) to mean the greatest common divisor of a and b. The positive integer c is said tob the greatest common divisor of a and b if

1. c is a divisor of a and of b
2. any divisor of a and b is a divisor of c

An equivalent definition is the following:

gcd(a,b)=max[k, such that k|a and k|b]

Because we require that the greatest common divisor be positive, gcd(a,b)=gcd(a,-b)=gcd(-a,b)=gcd(-a,-b). In general, gcd(a,b)=gcd(|a|,|b|).

gcd(60,24)=gcd(60,-24)=12

Also, because all nonzero integers divide 0, we have gcd(a,0)=|a|.

Greatest common divisor (CONT 1)

We stated that two integers are relatively prime if their only common positive integer factor is 1. This is equivalent to saying that a and b are relatively prime if gcd(a,b)=1.

8 and 15 are relatively prime because the positive divisors of 8 are 1,2,4, and 8, and the positive divisors of 15 are 1,3,5, and 15, so 1 is the only integer on both lists.

Finding the greatest common divisor

Euclid's algorithm is based on the following theorem: For any nonnegative integer a and any positive integer b,

gcd(a, b)=gcd(b, a mod b)   (4.3)

gcd(55,22)=gcd(22, 55 mod 22) = gcd(22,11) = 11

To see, that (4.3) works, let d=gcd(a,b). Then, by the definition of gcd, d|a and d|b. For any positive integer b, a can be expressed in the form

$a = kb+r \equiv r \bmod b$

a mod b = r

with k, r integers. Therefore, (a mod b) = a-kb for some integer k. But because d|b, it also divides kb. We also have d|a. Therefore, d|(a mod b). This shows, that d is a common divisor of b and (a mod b). Conversely, if d is a common divisor of b and (a mod b), then d|kb and thus d|[kb+(a mod b)], which is equivalent to d|a. Thus, the set of common divisors of a and b is equal to the set of common divisors of b and (a mod b). Therefore, the gcd of one pair is the same as the gcd of the other pair, proving the theorem.

Equation (4.3) can be used repetitively to determine the greatest common divisor:

gcd(18,12)=gcd(12,6)=gcd(6,0)=6

gcd(11,10)=gcd(10,1)=gcd(1,0)=1

Euclid's algorithm makes repeated use of (4.3) to determine the greatest common divisor, as follows. The algorithm assumes a>b>0. It is acceptable to restrict the algorithm to positive integers because gcd(a,b) = gcd(|a|,|b|)

EUCLID'S ALGORITHM

EUCLID(a,b)

1. A:=a; B:=b
2. if B=0 return A=gcd(a,b)
3. R=A mod B
4. A:=B
5. B:=R
6. goto 2

The algorithm has the following progression:

A1=B1xQ1+R1
A2=B2xQ2+R2
A3=B3xQ3+R3

To find gcd(1970,1066)

1970=1x1066+904	*gcd(1066,904)*
1066=1x904+162	*gcd(904,162)*
904=5x162+94	*gcd(162,94)*
162=1x94+68	*gcd(94,68)*
94=1x68+26	*gcd(68,26)*
68=2x26+16	*gcd(26,16)*
26=1x16+10	*gcd(16,10)*
16=1x10+6	*gcd(10,6)*
10=1x6+4	*gcd(6,4)*
6=1x4+2	*gcd(4,2)*
4=2x2+0	*gcd(2,0)*

Therefore, gcd(1970,1066)=2

This process should terminate, otherwise we would get an endless sequence of positive integers, each one is strictly smaller than the one before, and this is clearly impossible.