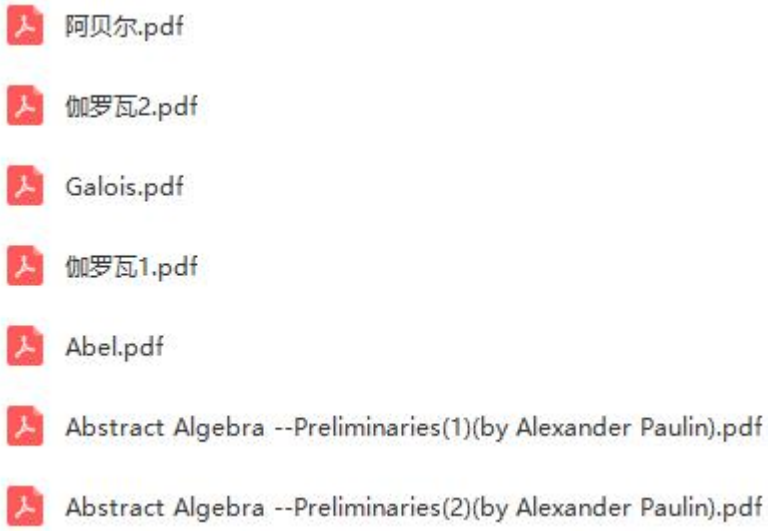
Assignments 10.1

一、阅读（Reading）

1. 阅读教材.

2. 课外阅读：



二、问题解答（Problems）

1. 教材第七章习题：题 2、6、7、8、10、11.

2. Let m and n be two integers with m < n. Let A = {m, m + 1, ... , n}, and let “min” be the function that returns the smaller of its two arguments. Does min have a zero（零元）? Identity（单位元）? Inverses（元素有逆元）? If so, describe them.

3. If <A;+>is a algebraic structure, where the binary operation + is associative, and <A;+>has an identity, and its element has an inverse, then <A;+> is called a group(群).

A ring(环) is an algebra with the structure<A; +, *>, where <A;+> is a commutative group(交换群, i.e. , <A;+> is a group and the operation + is commutative) , <A; *> is a monoid (独异点/单位半群, the identity element property is not required by some authors), and the operation * distributes over + from the left and the right（即*对+满足分配律）.

If <A; +, *> is a ring with the additional property that <A − {0}; *>is a commutative group, then it’ s called a field(域). Finite field, also known as Galois Field(named after Evariste Galois), refers to a field in which there exists finitely many elements. The most popular and widely used application of Galois Field is in Cryptography(密码学). Since each byte of data are represented as a vector in a finite field, encryption and decryption using mathematical arithmetic is very straightforward and is easily manipulable.

Now, let N_5 = {0, 1, 2, 3, 4}, and let $+_5$ and $*_5$ be the two operations of addition mod 5（求和后再模 5 求余数） and multiplication mod 5（求乘积后再对 5 求余数）, respectively. Please show that <N_5; $+_5$, $*_5$>is a field.

4. (定义满足某些性质的二元运算) Let A = {a, b}. For each of the following problems, find an operation table satisfying the given condition for a binary operation ○ on A.

a. <A; ○> is a group（群的定义请参考第 3 题）.

b. <A; ○> is a monoid but not a group.

c. <A; ○> is a semigroup(半群) but not a monoid.

三、项目实践（Programming）(Optional)

1. 编程实现：给定某集合与运算，判定其是否为代数结构，是否满足结合律、交换律，是否存在幂等元、单位元，元素是否可逆.