Prime Semigroups and Prime Groups

Shao-chang Lin

I. Introduction

The purpose of this article is to define a prime semigroup as well as a prime group according to the traditional definition for prime numbers. And from these definitions we establish a special relation between them.

II. Preliminaries

1. Prime semigroups

By a semigroup, we mean a nonempty set X with an associative binary operation, i.e.:

i) Any two elements $x,y\in X$ imply $xy\in X$.

ii) For any $x,y,z\in X$, $(xy)z=x(yz)$.

A semigroup is said to be finite if the number of elements of it is finite, otherwise, it is infinite. In particular, a semigroup which contains only one element is said to be trivial,

For any semigrotp X, the following properties hold true:

(1.1) For any $a\in X$, we have

$a^m a^n=a^{m+n}$ and $(a^m)^n=a^{mn}$,

where m and n are any posititve integers.

(1.2) If $a=b$ then $ca=cb$ and $ac=bc$, where $a,b,c\in X$.

In fact, a nonempty subset A of a semigroup X may happen to be a semigroup under the same operation. In this case, we say that A is a subsemigroup of X. In particular, any semigroup is a subsemigroup of itself.

From the above definition and (1.1), we can easily prove the following lemma:

Lemma (1.1). Let X be a semigroup. Then for any $x\in X$, the subset $A=\{x^k|k=1,2,3,...\}$ is a subsemigroup of X. In particular, $B=\{x^k|k=2,3,4,...\}$ is also a subsemigroup of X.

Next, let us consider a particular element which may occur in a semigroup X. By an idempotent, we mean an element $a\in X$ such that $a^2=a$. In general, it is possible that a semigroup may contain more than one idempotent.

Lemma (1.2). The element u is an idempotent of a semigroup X if and only if $\{u\}$ is a trivial subsemigroup of X.

Theorem (1.1) Every finite semigroup X contains an idempotennt.

Proof: We prove this by finite induction. If X is trivial, then from lemma (1.2) we can prove that the only element of X is an idempotent of X. Next, assume that every finite semigroup, whose number of element is less than n, contains an idempotent. Now, we shall try to prove that under this assumption a semigroup X of order n (containing n elements) also contains an idempotent. For this purpose, let $x\in X$. By lemma (1.1), it foollows that:

$$A=\{x^k \mid k=2,3,4,\ldots\}$$

is a subsemigroup of X.

Let us consider the following possible cases:

1) If $x\notin A$, then A is a proper subsemigroup of X whose order is less then n. By assumption, A must contain an idempotent. It follows immediately that X has an idempotent.

2) Otherwise, $x=x^k$ for some $k\geqslant 2$. If $k=2$ then $x=x^2$, so x is an idempotent of X. When $k>2$ we have

$$x^{k-1}x^{k-1}=x^{2k-2}=x^kx^{k-2}=xx^{k-2}=x^{k-1}.$$

This implies that x^{k-1} is an idempotent of X. Hence we complete this theorem. ‖

Definition (1). *A semigroup is said to be prime if and only if it has only trivial subsets and itself as its subsemigroups. In other words, a prime semigroup has no proper subsemigroup other than trivial subsemigroups and itself.*

2. Prime Groups

By a group, we mean a semigroup X which satisfies the following two conditions:

i) There exists a unique element $e\in X$ such that

$$ex=xe=x \text{ for every } x\in X,$$

ii) For every $x\in X$, there is a unique element $x^{-1}\in X$ such that

$$x^{-1}x=xx^{-1}=e.$$

*For convenience, define $x^0=e$.

According to the definition of groups, any group is a semigroup. But the converse is not true. We say that a group is finite if it is a finite semigroup, otherwise, it is said to be infinite.

For any group X, the following properties hold true:

(2.1). For any $a\in X$, we have

$$a^ma^n=a^{m+n} \quad \text{and} \quad (a^m)^n=a^{mn},$$

where m and n are any integers.

(2.2). Let a,b,c, be any elements in X. Then

$$a=b \text{ iff } ca=cb \text{ and } ac=bc.$$

In fact, a subsemigroup A of a semigroup X may happen to be a group. In this case, we say that A is a subgroup of X. In particular, if X is a group then {e} and X are both subgroups of X. We call them a trivial subgroup and the improper subgroup of X respectively. The other subgroups of X (if any) are called proper subgroups.

Lemma (2.1). Let X be a group. Then the element e is the only idempotent in X.

Proof: Assume that a is an idempotent of X. Then by poperty (2.1), it follows that:

$$a=a^2a^{-1}=aa^{-1}=e. \text{ ‖}$$

From Lemmas (1.2) and (2.1), we obtain:

Lemma (2.2.). Every group has one and only one trivial subsemigroup, that is {e}.

Theorem (2.1). Every subsemigroup of a finite group X is a subgroup of X.

Proof: Let A be a subsemigroup of X. Then A is finite. By theorem (1.1). and lemma (2.1), it follows readiy that A contains e, the neutral element of X.

Next, we have to prove that every $x\in A$ implies $x^{-1}\in A$. Clearly $e^{-1}=e\in A$. Let $x\in A$ and $x\neq e$. Since X is finite, there must exist a positive integer $k>1$ such that $x^k=e$. For if not, then $x^n\neq e$ for every positive integer n. But X is a finite group, so we can find two powers of x such that $x^p=x^q$, where $p>q$. By property (2.2), it follows that $x^{p-q}=e$, contradicting our assumption. By property (2.1), we have

$$x^{-1}=x^{k-1}\in A,$$

Hence we complete this proof. ‖

Definition (2). *A group is called a prime group if and only if it is finite and has only {e} and itself as its subgroups. In other words, a prime group is a finite group which has no proper subgroup other than the trivial subgroup and itself.*

In particular, a trivial group is considered as a prime group.

III. Theorem. ***A semigroup is prime if and only if it is a prime group or has at most two elements.***

Proof: We shall prove this theorem in two parts:

1. Necessity. Let X be a prime semigroup. To prove that X is a prime group or has at most two elements, one of the methods is to consider the following two possible cases:

1) If every element of X is an idempotent, then for any two distinct elements $a, b\in X$, there are only three cases which the product of a and b may occur. That is:

i) If the product of a and b is equal to either a or b, then {a, b} is a subsemigroup of X. It follows readily that {a, b} =X.

ii) Assume ab=a, (or=b) and ba=c for some $c\in X$. Then

$$ac=a(ba)=(ab)a=aa=a^2=a \text{ and}$$
$$ca=(ba)a=ba^2=ba=c.$$

From i), it follows that {a, c} =X.

iii) Assume ab=c and ba=d for some $c,d\in X$. Then

$$da=(ba)a=ba^2=ba=d.$$

From i) and ii) it follows that {a,d} =X

Hence, in the case 1), X can possess at most two elements.

2) Otherwise, let x be an element of X which is not an idempotent. Then $x^2\neq x$. By lemma (1.1), we know that

$$A=\{x^k\,|\,k=1,2,3,\ldots\}$$

is a subsemigroup of X which contains at least two distinct elements, i. e., x and x^2. Since X is prime, so A must be equal to X.

Furthermore, there exist two powers of x in A which represent the same element in X. For if not, then all powers of x are distinct and A is infinite. Thus, the subsemigroup

$$B=\{x^k\,|\,k=2,3,4,\ldots\}$$

is a proper subsemigroup of X. This is contradictory to our assumption that X is

prime.

Now, let m be the smallest integer such that $x^r=x^m$ for some $r>m$ and consider the following possible cases for r:

i) If $r=m+1$, then m must be greater than 1, (since $x\neq x^2$), and by property (1.1) we have

$$x^{r+p}=x^px^r=x^px^m=x^{p-1}x^{m+1}=x^{p-1}x^m=\ldots=xx^m=x^{m+1}=x^m,$$

i.e. $x^s=x^m$ for all $s\geqslant m+1$..... (*1)

Since

$$2m-1=(m+1)+(m-2)\geqslant m+1,$$

so from (*1) there results

$$x^{m-1}x^m=x^mx^{m-1}=x^{2m-1}=x^m.$$

It follows that $\{x^{m-1}, x^m\}$ is a subsemigroup of X. Hence $\{x^{m-1}, x^m\}=X$. This proves that X contains at most two elements.

ii) Otherwise, the subset

$$C=\{x^{m+i}\mid i=0,1,2,\ldots,r-1\}$$

contains at least two distinct elements, i,e.,$x^m\neq x^p$ if $m<p<r$. Now, we will try to prove that C is a subsemigroup of X. For this purpose, let $r=m+d$ for some d such that $1<d<r$. As we know, for a given positive integer p there exists a unique positve integer k, $0\leqslant k<d$, such that $p=qd+k$. It follows that

$$x^{r+p}=x^px^r=x^{k+qd}x^m=x^{k+(q-1)d}x^{m+d}=x^{k+(q-1)d}x^m=\ldots=x^kx^m=x^{m+k},$$

i.e. $x^s\in C$ for all $s\geqslant r$..... (2*)

From (2*), it is easily seen that C is a subsemigroup of X. Since X is prime, it follows that $C=X$ and $x=x^k$ for some $x^k\in C$. Hence, m must be equal to 1. Therefore, we have

$$X=\{x,x^2,x^3,\ldots,x^{r-1}\} \text{ and } x^r=x.$$

Finally, we complete this proof by proving X is a finite group. Since

i) $x^{r-1}x^k=x^kx^{r-1}=xx^{k-1}=x^k$, $k=1,2,3,\ldots,r-1$, this proves that x^{r-1} is the neutral of X.

ii) For any positive integer p, $1\leqslant p<r-1$, there exists a unique positive integer q, such that $p+q=r-1$, where $1\leqslant q<r-1$. It follows that

$$x^qx^p=x^px^q=x^{p+q}=x^{r-1},$$

this proves that every element of X has a unique inverse.

Hence X is a finite group. From definitions (1), (2) and theorem (2.1), it follows immediately that X is a prime group.

2. Sufficiency.

If X is a semigroup which contains only two elements, then the result is obvious.

Assume that X is a prime group. Then it is finite. If A is a subsemigroup of X, then by theorem (2.1) and definition (2), A must be equal to either the trivial subgroup or X. Hence X is a prime semigroup according to definition (1). ‖

REFERENCE

1. Sze-tsen Hu, Elements of Modern Algebra (1965), chapters II-III
2. Dennis B. Ames, An Introduction to Abstract Algebra (1969) pp. 29-63
3. Jacobson, Lecture of Abstract Algebra (1951), pp 15-48

質半群與質群

林韶璋

本文乃依傳統上對質數所下之定義而定義質半羣與質羣。進而討論此兩羣間之特殊關係。

Prime Semigroups and Prime Groups

hao-chang Lin

The purpose of this article is to define a prime semigroup as well as a prime group according to the traditional definition for prime numbers. And from these definitions we establish a special relation between them.