21 - 341

Linear Algebra I

## Some Additional Remarks on Fields

**A. Ordered Fields**: Let  $\mathbb{F}$  be a field. By a *positive half* or *positive part* for  $\mathbb{F}$ , we mean a set  $\mathbb{P} \subset \mathbb{F}$  satisfying (1) and (2) below.

(1)  $\forall \alpha, \beta \in \mathbb{P}, \ \alpha + \beta \in \mathbb{P} \text{ and } \alpha \beta \in \mathbb{P}.$ 

(2) For each  $\alpha \in \mathbb{F}$  exactly one of the following three conditions holds:  $\alpha \in \mathbb{P}, \ \alpha = 0, \ -\alpha \in \mathbb{P}.$ 

By an *ordered field* we mean a field together with a positive half. A given field may have no positive half, exactly one positive half, or more than one positive half. These possibilities are illustrated in Assignment 1.

**B.** The Characteristic of a Field: Let  $\mathbb{F}$  be a field. Given  $\alpha \in \mathbb{F}$  and  $n \in \mathbb{Z}^+$ , we can define  $n\alpha \in \mathbb{F}$  by induction as follows:  $1\alpha = 1$ ; given  $k \in \mathbb{Z}^+$  and assuming  $k\alpha$  has been defined, we put  $(k+1)\alpha = k\alpha + \alpha$ . Let  $S = \{n \in \mathbb{Z}^+ | n1 = 0\}$ . If  $S = \emptyset$ , we say that  $\mathbb{F}$  has *characteristic zero*. If  $S \neq \emptyset$ , we define the *characteristic* of  $\mathbb{F}$  to be the smallest element of S. It can be shown that the characteristic of a field is either zero or prime.

C. The Field  $\mathbb{Z}_p$ : Let  $n \in \mathbb{Z}^+$  be given and let

$$\mathbb{Z}_n = \{0, 1, 2, \dots n - 1\}$$

equipped with addition and multiplication modulo n. It can be shown that  $\mathbb{Z}_n$  is a field if and only if n is prime.

**D. General Finite Fields**: It can be shown that if  $\mathbb{F}$  is a finite field then the number of elements of  $\mathbb{F}$  is of the form  $p^n$  for some prime number p and some  $n \in \mathbb{Z}^+$ . It can be also shown that given any prime p and  $n \in \mathbb{Z}^+$  there is a field having exactly  $p^n$  elements. Moreover, for any field having exactly  $p^n$  elements (where p is prime and  $n \in \mathbb{Z}^+$ ) the characteristic is p.