Chapter 1

Vector Spaces

A subset of W of $\mathbb{R}^n$ is a *subspace* if it has the following proerties:

(a) If $w, w' \in W$, then $w + w' \in W$

(b) If $w \in W$, $c \in \mathbb{R}$, then $cw \in W$

(c) The zero vector is in W

Note that (c) seems to be a special case of (b), by putting $c = 0$. However, it is (c) which ensures that W is not the empty set.

1.1 Fields

The quintessential model for a field is the set of all complex numbers $\mathbb{C}$.

Definition 1. *A* field *F is a set together with two composition laws*

$$F \times F \xrightarrow{+} F \quad \text{and} \quad F \times F \xrightarrow{\times} F \tag{1.1}$$

called addition*: $a + b \mapsto a + b$ and* multiplication*: $a \times b \mapsto ab$, which satisfy these axioms*

(i) F with addition, written as F^+, is an abelian group,
(ii) $F/\{0\}$ with multiplication, written as $F^\times$, is an abelian group,
(iii) distributive law: *For all $a, b, c \in F$, we have $a(b + c) = ab + ac$.*

Note that axiom (iii) relates multiplication and addition.
A very interesting example of a field is

$$\mathbb{F}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\} = \mathbb{Z}/\mathbb{Z}_p,$$

where p is a prime number.

Lemma 1. *The characteritic of any field F is either zero or a prime number.*

Proof. Assume that the characteristic m is neither zero nor prime. Then, it can be written as $m = rs$ for some positive integers r, s. Since we have

$$0 = \overbrace{1 + \cdots + 1}^{m \text{ times}} = \overbrace{1 + \cdots + 1}^{r \text{ times}} + \cdots + 1.$$

Writing $\overbrace{1+\cdots+1}^{r \text{ times}} = a$, we get

$$0 = \overbrace{a+\cdots+a}^{s \text{ times}} = a(\overbrace{1+\cdots+1}^{s \text{ times}})$$

Now, either

$$\overbrace{1+\cdots+1}^{s \text{ times}} = 0 \quad \text{or} \quad a = \overbrace{1+\cdots+1}^{r \text{ times}} = 0.$$

In either case, we have a contradiction. □

1.2 Problems

1.8

Let p be a prime integer.

(a) Fermat's theorem: $a^p \equiv a \mod p$ for every integer a.
This is a direct consequence of the fact that $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$.

(b) Wilson's theorem: $(p-1)! \equiv -1 \mod p$.
The case with $p = 2$ is trivial. Let $p > 2$, which is odd. Let a be a primitive root of $\mathbb{F}_p^\times$. We have

$$\begin{aligned} \{1, \ldots, p-1\} &= \{a^1, \ldots, a^{p-1}\} \\ \implies (p-1)! &= a^1 \cdots a^{p-2} a^{p-1} \\ &= a^{\frac{p(p-1)}{2}} \end{aligned}$$

Since, $a^p \equiv a \mod p$ (by Fermat's theorem), then $(a^p)^{(p-1)/2} \equiv a^{(p-1)/2} \mod p$.

For some integer x, if we have $x^2 \equiv 1 \mod p$, then

$$\begin{aligned} x^2 - 1 = (x-1)(x+1) &\equiv 0 \mod p \\ \implies x \equiv 1 \mod p \quad \text{or} \quad x &\equiv -1 \mod p \end{aligned}$$

If $x = a^{(p-1)/2}$, then $x = 1$ would mean that a is not a primitive root, which is a contradiction. So, $a^{(p-1)/2} \equiv -1 \mod p$. Thus,

$$\begin{aligned} (p-1)! = a^{\frac{p(p-1)}{2}} &\equiv a^{\frac{p-1}{2}} \mod p \\ &\equiv -1 \mod p \end{aligned}$$

□