Countability:

A set X is called Countable if there's a bijection $X \longrightarrow Y$ for $Y \subset \mathbb{N}$

Ex: $\mathbb{Z}, \mathbb{Q}, \mathbb{Z}[x]$

$\mathbb{R}$ is not countable

Any finite set is countable

Prop: Finite products of countable sets

are countable.

Prop: Countable unions of countable sets are countable. i.e. if X_i are countable, so is

$$\bigcup_{i=1}^{\infty} X_i.$$

Hint for problem 3:

First show that $\mathbb{R}$ is infinite dimensional

over $\mathbb{Q}$. Then try and use second prop.

Hint for problem 4:

Use Zorn's lemma to

Construct maximal

$\mathbb{Q}$-ind. subset of

spanning set and

show it's a basis.

Want to show that

either $n \cdot 1 \neq 0$

$\underbrace{1+1+\cdots+1}_{n \text{ times}}$ for any n

OR $p \cdot 1 = 0$

for some prime p.

Ex: $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$

$p \cdot 1 = 0$

Def: The characteristic of a field F is the smallest $n \geq 1$ s.t. $n \cdot 1 = 0$

If no such n exists, $\text{char}(F) = 0$.

Hint for 1:

Work with characteristic.

(i.e. use smallest such n). Use the fact that integers are

products of prime.

Finite fields

$$\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$$

p prime

addition/multiplication

are "mod p": i.e.

take remainder after

division by p.

Ex: $\mathbb{F}_5$

$4+4 = 3$ in $\mathbb{F}_5$

$4+4 = 8$

$5 \overline{)8}\ 1$ remainder 3

$4 \cdot 3 = 12$

$4 \cdot 3 = 2$ in $\mathbb{F}_5$ bc

$12 = 10 + 2$

Ex: $\mathbb{F}_4 = \{0, 1, \alpha, 1+\alpha\}$

$1+1 = 0$

$\alpha + \alpha = 0$

$\alpha^2 + \alpha + 1 = 0$

if F is a finite field,

HW1 #1 shows that

$\text{Char}(F) = p$ for prime

p.

So F is an $\mathbb{F}_p$-vector space.

Since F is finite, it's finite dimensional

$\Rightarrow F \cong \mathbb{F}_p^n$

$W \subset V$

V/W

$= \{ v + W : v \in V \}$

$(v+W) + (v'+W) = (v+v') + W$

$c \cdot (v+W) = (c \cdot v) + W$

Prop: $\dim(V/W)$

$= \dim(V) - \dim(W)$

Proof:

Start with $\{w_1, \ldots, w_k\}$

a basis of W.

Expand to a basis

$\{w_1, \ldots, w_k, e_1, \ldots, e_l\}$

of V.

Claim: $\{e_1+W, \ldots, e_l+W\}$ is a basis for V/W.

Proof:

Suppose

$$c_1(e_1+W)+\cdots+c_l(e_l+W) = 0+W$$

$\Rightarrow$

$$(c_1e_1+\cdots+c_le_l)+W = 0+W$$

$\Rightarrow$

$c_1 e_1 + \cdots + c_l e_l = w$ for some $w \in W$.

$$w = d_1 w_1 + \cdots + d_k w_k$$

$$c_1 e_1 + \cdots + c_l e_l - d_1 w_1 - \cdots - d_k w_k = 0$$

$\Rightarrow$ all $c_i, d_i = 0$

b/c $\{e_1, \ldots, e_l, w_1, \ldots, w_k\}$

a basis.

To see it spans V/W,

Pick $v+W \in V/W$

$$v = c_1 e_{l+1} + \cdots + c_l e_l + d_1 w_1 + \cdots + d_k w_k$$

$$v + W$$

$$=$$

$$(c_1 e_{l+1} + \cdots + c_l e_l + d_1 w_1 + \cdots + d_k w_k) + W$$

$$=$$

$$c_1(e_{l+1}+W) + \cdots + c_l(e_l + W)$$

$$+ \cdots + d_1(\omega_1 + W) + \cdots + d_k(\omega_k + W)$$

$$0 + W \quad \text{b/c} \quad \omega_i \in W$$

$$= c_1(e_1 + W) + \cdots + c_\ell(e_\ell + W)$$

So we're done.

Proof #2:

Define $T: V \to V/W$

$T(v) = v + W$.

T is a linear transformation

and T is surjective

$$\dim(V) = \dim \ker T + \dim \operatorname{im} T$$

$$= \dim \ker T + \dim V/W$$

$$\ker(T) = W$$

$$\dim V = \dim W + \dim V/W$$

□

$$\ker(T) = \{ v : T(v) = 0 \text{ in } V/W \}$$

$0 \perp W$

$v + W = 0 + W$

$\Leftrightarrow$

$v \in W$