1.2 Posets and Zorn's Lemma

A set Σ is called **partially ordered** or a **poset** with respect to a relation $\leq$ if

(i) **(reflexivity)**

$$(\forall \sigma \in \Sigma) \qquad \sigma \leq \sigma \ ;$$

(ii) **(antisymmetry)**

$$(\forall \sigma, \tau \in \Sigma) \qquad \sigma \leq \tau \leq \sigma \quad \Longrightarrow \quad \sigma = \tau \ ;$$

(iii) **(transitivity)**

$$(\forall \rho, \sigma, \tau \in \Sigma) \qquad \rho \le \sigma \le \tau \quad \Longrightarrow \quad \rho \le \tau \ .$$

Let $X \subseteq \Sigma$ where Σ is a poset.

Call X a **chain** or say that X is **totally ordered** if

$$(\forall x, y \in X) \qquad x \le y \quad \text{or} \quad y \le x \ .$$

"everything is comparable"

Call $\sigma \in \Sigma$ an **upper bound** for X if

$$(\forall x \in X) \qquad x \leq \sigma \ .$$

Call $\sigma \in \Sigma$ **maximal** if

$$(\forall \tau \in \Sigma) \qquad \sigma \leq \tau \quad \Longrightarrow \quad \sigma = \tau \ .$$

Examples:

(1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ are totally ordered with respect to the usual $\leq$, and all of these fail to have a maximal element.

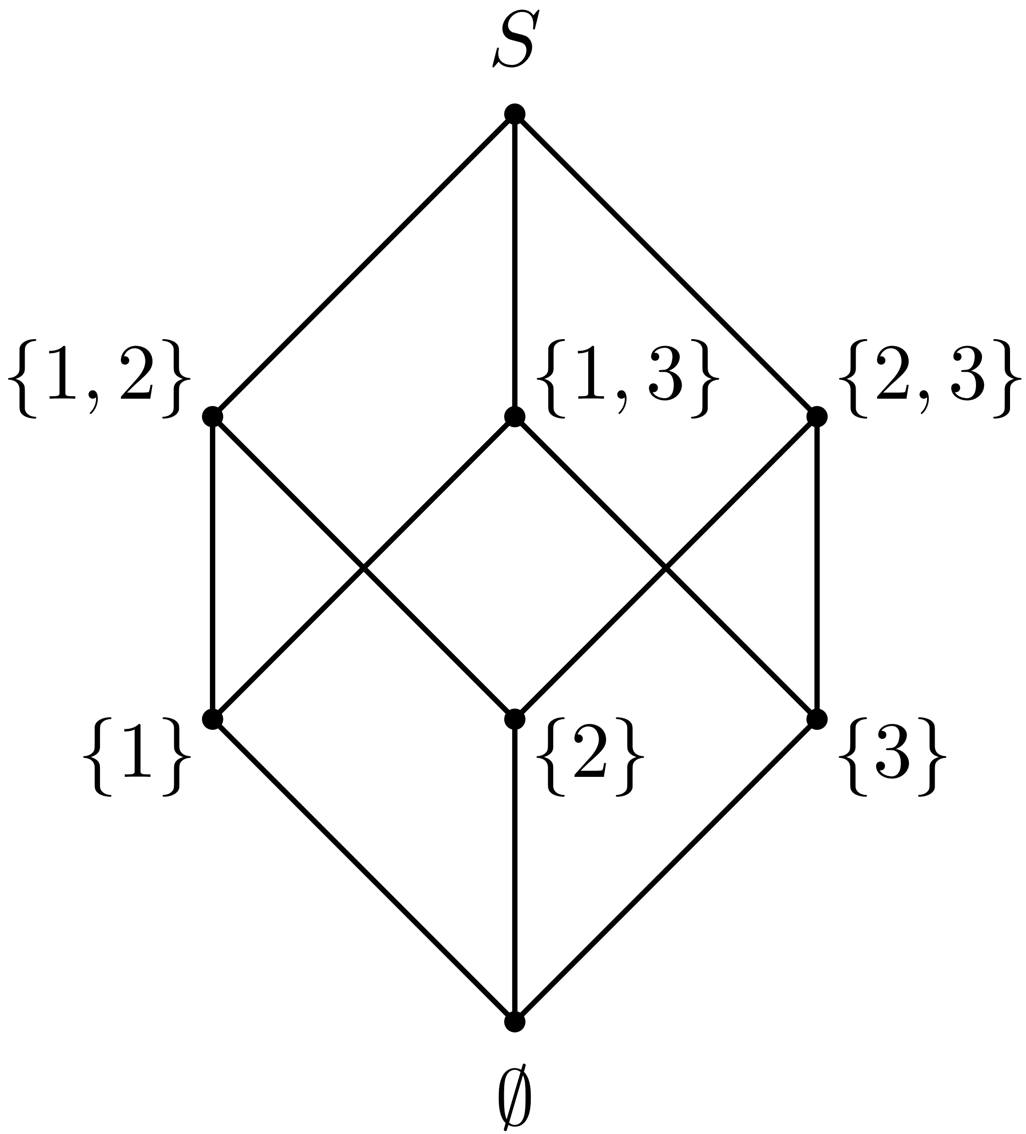
(2) Let S be a set and put

$$\Sigma \;=\; \mathcal{P}\,(S) \;=\; \{\, T \mid T \subseteq S \,\}\,,$$

the **power set** of S , which is a poset with respect to $\subseteq$, having S as **the** maximal element.

If $|S| > 1$ then $\mathcal{P}(S)$ is **not** totally ordered.

e.g. If $S = \{1, 2, 3\}$ then $\mathcal{P}(S)$ looks like


S
$\{1, 2\}$
$\{1, 3\}$
$\{2, 3\}$
$\{1\}$
$\{2\}$
$\{3\}$
$\emptyset$

The previous picture is called a **Hasse diagram**,

in which a line segment joins two nodes x and y if $x < y$ and there is no z for which $x < z < y$,

in which case we say y **covers** x .

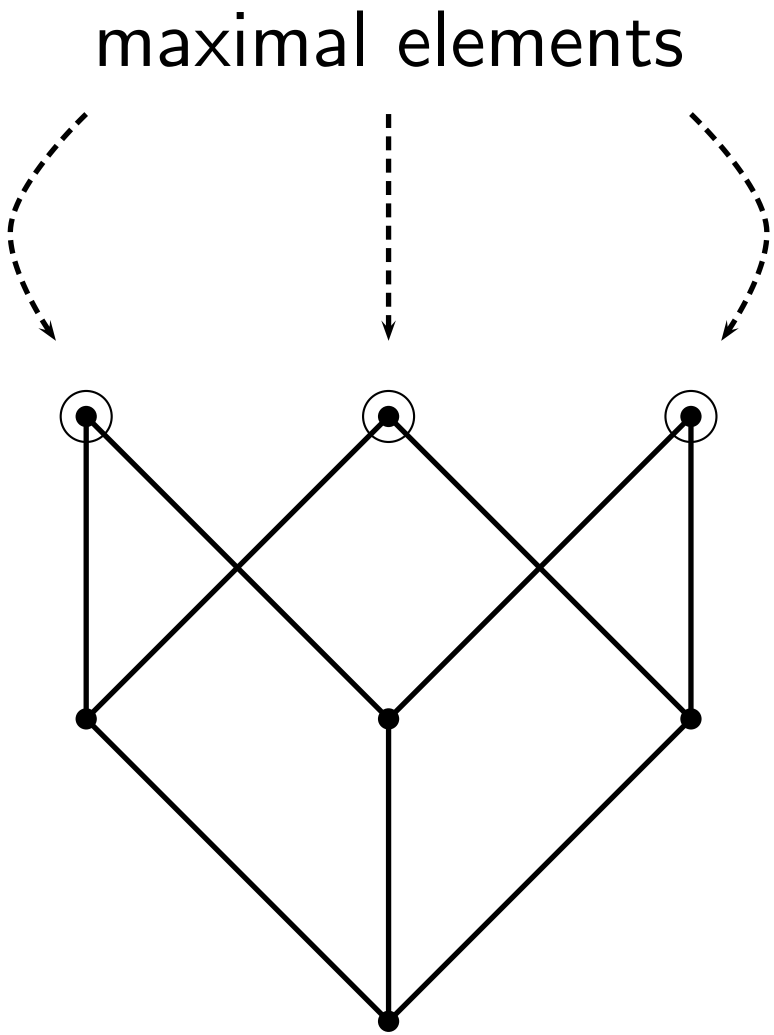
Now put

$$\Sigma' = \mathcal{P}(S) \setminus \{S\} .$$

Then Σ' is a poset with respect to $\subseteq$ (called a **sub**poset of Σ), but now Σ' has many maximal elements, namely

$$S \backslash \{x\} \qquad \text{where} \qquad x \in S .$$

e.g. if $S = \{1,2,3\}$ then Σ' looks like


maximal elements

Examples (continued):

(3) Let A be a ring and put

$$\Sigma = \{ I \mid I \lhd A ,\ I \neq A \} .$$

Then Σ is a poset with respect to $\subseteq$, and now the maximal elements of Σ are precisely the maximal ideals of A.

e.g. If $A = \mathbb{Z}_2$ then $\Sigma \cup \{A\}$ is the poset

If R, S are rings then define the **direct sum** to be

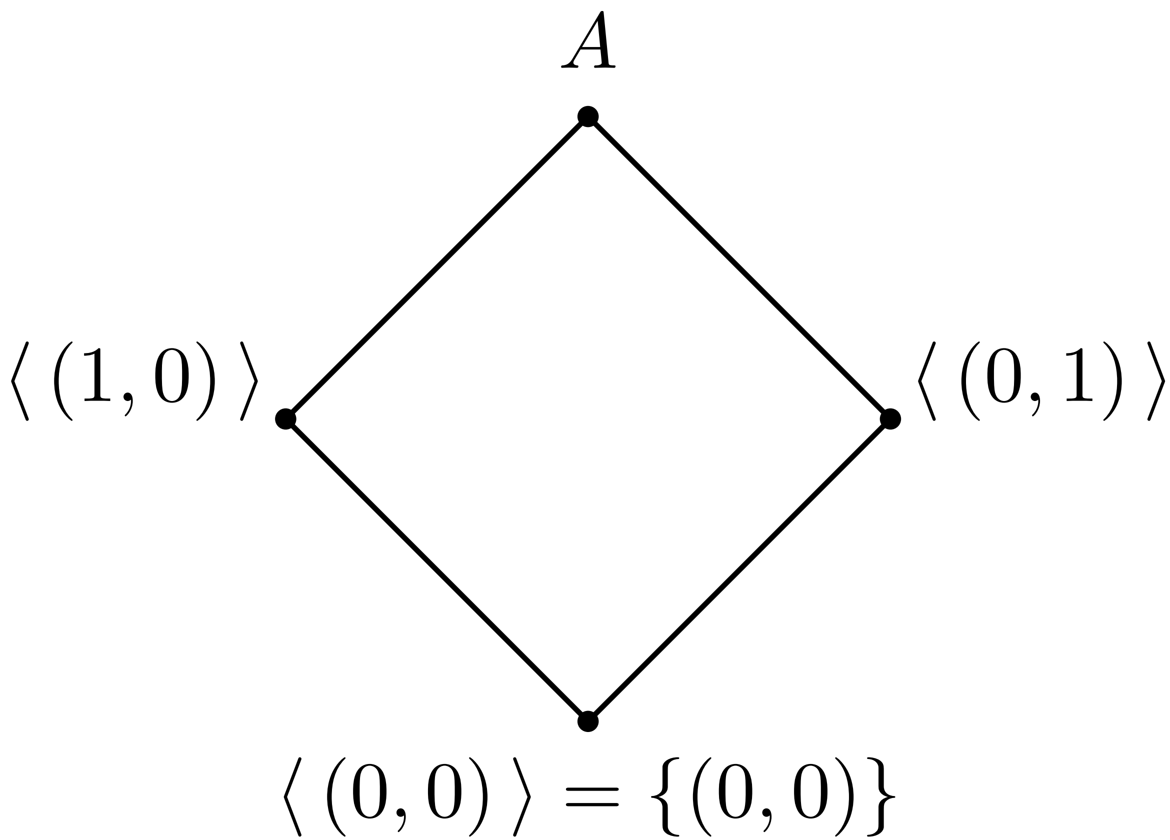
$$R \oplus S \;=\; \{\, (x, y) \;|\; x \in R\,,\;\; y \in S \,\}$$

with coordinatewise operations.

e.g. If

$$A = \mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{ (0,0),(0,1),(1,0),(1,1) \}$$

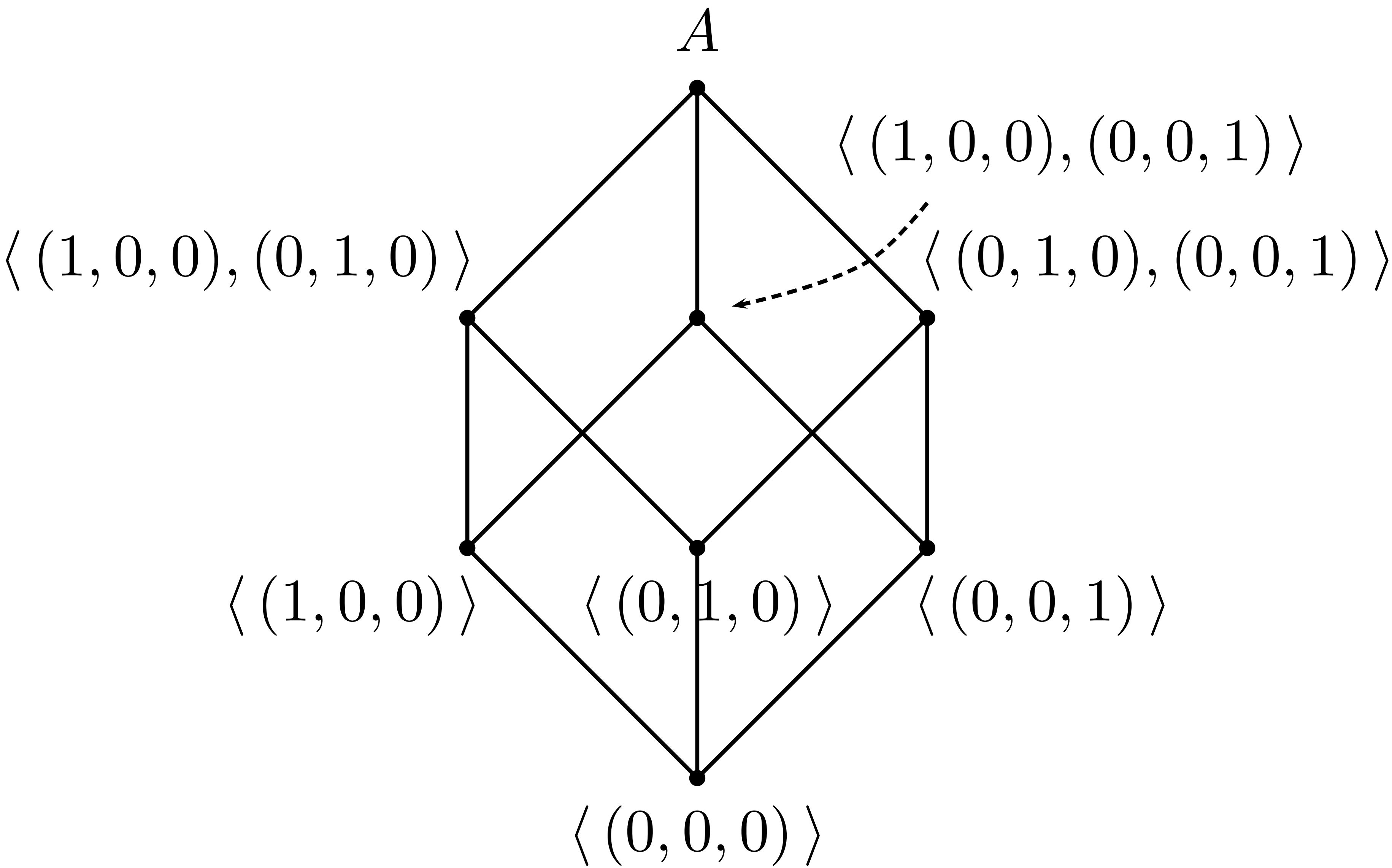
then $\Sigma \cup \{A\}$ is the poset



where $\langle\quad\rangle$ denotes "ideal generated by...".

The maximal ideals of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ are $\langle\,(0,1)\,\rangle$ and $\langle\,(1,0)\,\rangle$, both of which are rings with identity (!) isomorphic to $\mathbb{Z}_2$.

e.g. If $A = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ then $\Sigma \cup \{A\}$ is the poset



The maximal ideals are all isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Exercise: Prove that if A and B are rings and

$$I \ \lhd \ A \oplus B$$

then

$$I \ = \ C \oplus D$$

$$= \ \{ \ (x, y) \ \mid \ x \in C \ , \ \ y \in D \ \}$$

for some $C \lhd A$, $D \lhd B$.

Exercise: Draw the Hasse diagram for the poset of vector subspaces (under $\subseteq$) of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, regarded as a 2-dimensional vector space over the field $\mathbb{Z}_2$.

(Compare with the poset of **ideals** of the **ring** $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.)

A poset Σ is called **well-ordered** if Σ is totally ordered and

each nonempty subset of Σ has a least element.

e.g. $\mathbb{Z}^+$, $\mathbb{N}$ are, but $\mathbb{Z}$, $\mathbb{Q}^+$, $\mathbb{R}^+$, $\mathbb{Q}$, $\mathbb{R}$ are **not** well-ordered with respect to the usual $\leq$.

All finite totally ordered sets are well-ordered.

Exercise: Let Σ be a nonempty alphabet given some total order $\leq$.

Define the **lexicographic** or **dictionary** order on $\Sigma^* = \{$ words over Σ $\}$ by $x_1 \ldots x_m < y_1 \ldots y_n$ if, for some k such that $0 \leq k < n$,

$$(\forall i) \qquad 0 < i \leq k \implies x_i = y_i$$

$$\text{and} \qquad k+1 \leq m \implies x_{k+1} < y_{k+1} .$$

Verify that Σ^* is well-ordered iff $|\Sigma| = 1$.

We use the following result from set theory:

Zorn's Lemma: Let Σ be a nonempty poset such that every chain $\mathcal{C} \subseteq \Sigma$ has an upper bound in Σ. Then

Σ has a maximal element.

This is equivalent to the **Axiom of Choice**, the **Well-Ordering Principle**, and **Transfinite Induction**

(explained, for example, in "Naive Set Theory" by Halmos).

The **Well-Ordering Principle** says that every set can be well-ordered.

This is nontrivial; e.g. there is no known explicit well-ordering of $\mathbb{R}$.

Idea of proof of Zorn's Lemma:

(1) Start with any element $x_0 \in \Sigma$ and build a chain upwards

$$x_0 \ < \ x_1 \ < \ x_2 \ < \ \ldots$$

unless you reach a maximal element.

(2) This chain has an upper bound y_0 .

(3) Build a new chain upwards

$$y_0 < y_1 < y_2 < \dots$$

unless you reach a maximal element.

(4) Continue building a chain unless you reach a maximal element.

(5) Suppose "every element of Σ gets examined" yet the chain $\mathcal{C}$ continues to be built without bound. Then for all $z \in \Sigma$

$$(\exists x \in \mathcal{C}) \qquad x \not< z$$

(6) But $\mathcal{C}$ has an upper bound z_0 , so

$$(\forall x \in \mathcal{C}) \qquad x \leq z_0$$

contradicting (5).

(7) Hence (5) can't happen, so in the process of attempting to build such a chain $\mathcal{C}$ a maximal element must have been reached.

The "examining of every element of Σ" can be made precise if we assume Σ has been well-ordered.

Difficult (optional) exercise:

Prove that Zorn's Lemma and the Well-Ordering Principle are equivalent.

The following is a standard application of Zorn's Lemma:

Theorem: Every nonzero ring has a maximal ideal.

Proof: Let A be a nonzero ring and put

$$\Sigma \;=\; \{\, I \mid I \lhd A \,,\; I \neq A \,\} \,.$$

Then Σ is a poset with respect to $\subseteq$.

Also $\Sigma \neq \emptyset$ since $\{0\} \in \Sigma$.

Let $\mathcal{C} \subseteq \Sigma$ be a chain.

If $\mathcal{C} = \emptyset$ put $K = \{0\}$.

If $\mathcal{C} \neq \emptyset$ put

$$K = \bigcup_{\{I \in \mathcal{C}\}} I = \{ x \in A \mid (\exists I \in \mathcal{C}) \ x \in I \} .$$

We check that $K \lhd A$.

This is clear if $\mathcal{C} = \emptyset$, so suppose $\mathcal{C} \neq \emptyset$.

(i) $K \neq \emptyset$ since $0 \in K$.

(ii) Let $\boxed{x, y \in K \text{ , } z \in A \text{ .}}$ Then

$$x \in I \, , \quad y \in J \qquad (\exists\, I \, , \ J \ \in \mathcal{C}) \ .$$

But $\mathcal{C}$ is a chain, so $J \subseteq I$ or $I \subseteq J$.

If $J \subseteq I$ then $x - y \in I \subseteq K$, and if $I \subseteq J$ then $x - y \in J \subseteq K$. Thus

$$\boxed{x - y \in K \text{ .}}$$

Further $xz \in I \subseteq K$, so $xz \in K$.

By (i) and (ii), $K \triangleleft A$.

We check that $K \neq A$.

If $1 \in K$ then $1 \in I$ for some $I \in \mathcal{C}$, so $I = A$, contradicting that $I \in \Sigma$.

Hence $K \neq A$. Thus

$K \in \Sigma$ and clearly K is an upper bound for $\mathcal{C}$.

By Zorn's Lemma, Σ has a maximal element, which is a maximal ideal of A , and the theorem is proved.

Corollary: Let $I \lhd A$, $I \neq A$. Then there exists a maximal ideal of A containing I .

Proof: By the Theorem, since A/I is nonzero, A/I has a maximal ideal $\mathcal{J} = J/I$ for some $I \subseteq J \lhd A$.

But the maximality of $\mathcal{J}$ implies the maximality of J, and we are done.

Corollary: Every nonunit in $A \neq \{0\}$ is contained in a maximal ideal of A.

Proof: If $x \in A$ is a nonunit then $xA \lhd A$ but $xA \neq A$, so, by the previous Corollary,

there exists a maximal ideal J of A containing xA ,

so certainly $x \in J$, and we are done.

Remark: Consider the case when $A \neq \{0\}$ satisfies the **ascending chain condition (a.c.c.)**

(we call A **noetherian** – see **Part 3**), that is, if

$$I_1 \subseteq I_2 \subseteq \ldots$$

is an ascending chain of ideals of A then

$$I_n = I_{n+1} = \ldots \qquad (\exists n \geq 1) .$$

Then Zorn's Lemma can be avoided in the proof of the Theorem:

- start with $I_1 = \{0\}$;

- if I_1 is not maximal then

$$I_1 \subset I_2 \lhd A , \qquad (\exists I_2 \neq A) ;$$

- continuing, either one reaches a maximal ideal, or one produces a strictly ascending chain

$$I_1 \subset I_2 \subset I_3 \subset \ldots$$

which is impossible by the a.c.c.;

- hence one finds a maximal ideal of A .