7. Nilpotent and nil ideals, Zorn's lemma (Chapters 10.5 – 10.6)

R – ring
I – right or left ideal in R

Definition 7.1. (1) I is called <u>nil</u> if every element $x \in I$ is nilpotent, i.e. $x^n = 0$ for some $n > 0$.
(2) I is called <u>nilpotent</u> if $I^n = 0$ for some $n > 0$.

Example 7.2. (1) Every nilpotent right or left ideal is nil since $x^n \in I^n$ for every $x \in I$.
(2) Let $R = \mathbb{Z}_4$ and $I = (2) = \{0, 2\}$. Then $I^2 = (0)$ and so I is nilpotent and nil.
(3) Let F be a field and $R = M_n(F)$. Assume I is a nilpotent right ideal of R, that is $I^k = 0$ for some $k > 0$. Then

$$(RI)^k = (RI)\cdots(RI) = R\overbrace{(IR)\cdots(IR)}^{k-1 \text{ terms}}I \subseteq R\overbrace{I\cdots I}^{k-2 \text{ terms}}I = RI^k = (0).$$

Since (RI) is a two-sided ideal in $M_n(F)$, we have that $(RI) = (0)$ or $(RI) = R$ by Theorem 3.4(3). Since (RI) is nilpotent, we conclude that $(RI) \neq R$ (because $1 \in R$ is not nilpotent). Hence $(RI) = (0)$ or $RI = (0)$. Then if $a \in I$, we have that $a = 1 \cdot a \in RI = (0)$ and so $a = 0$. We conclude that the only right or left nilpotent ideal of $M_n(F)$ is (0).
(4) Assume R is commutative. Then the set of all nilpotent elements in R is a nil ideal (exercise).
(5) There exist nil ideals which are not nilpotent. Let p be a prime number and assume

$$R = \bigoplus_{i>0} \mathbb{Z}/(p^i).$$

Then R is commutative and so the set I of all nilpotent element in R is a nil ideal by (4). Let $k>0$. Then

$$x_k = (0+(p), 0+(p^2), \dots, 0+(p^k), p+(p^{k+1}), 0+(p^{k+2}), \dots) \in R$$

satisfies $x_k^{k+1}=0$ and so $x_k \in I$, but $x_k^k \neq 0$. Hence for every $k>0$, there exists $x = x_k \in I$ such that $x^k \neq 0$ and so I is not nilpotent.

Definition 7.3. (1) A <u>partially ordered set (poset)</u> is a set S with a binary relation $\leq \subseteq S \times S$ such that for all $a,b,c \in S$ we have

- $a \leq b$ and $b \leq a \Rightarrow a=b$ (<u>antisymmetric</u>),
- $a \leq a$ (<u>reflexive</u>),
- $a \leq b$ and $b \leq c \Rightarrow a \leq c$ (<u>transitive</u>).

(2) A <u>chain</u> C in a poset $(S, \leq)$ is a subset $C \subseteq S$ such that if $a, b \in C$, then $a \leq b$ or $b \leq a$. An element $u \in S$ is an <u>upper bound</u> of C if $a \leq u$ for all $a \in C$. An element $m \in S$ is a <u>maximal element</u> of $(S, \leq)$ if $m \leq a$ for $a \in S$ implies $m = a$.

Zorn's lemma. Let $(S, \leq)$ be a nonempty poset. If every nonempty chain in S has an upper bound in S, then there exists a maximal element in S.

Zorn's lemma is equivalent to the axiom of choice and the well-ordering principle (in Zermelo–Fraenkel set theory). We need it to show for example the existence of a basis in every vector space.

<u>Theorem 7.4.</u> Assume R is unital. Then for every ideal I in R with $I \neq R$ there exists a maximal ideal M in R with $I \subseteq M$.

<u>Proof</u> Let $I \subseteq R$ be an ideal with $I \neq R$. Set
$S := \{ J \text{ ideal in } R \mid I \subseteq J \text{ and } J \neq R \}$.
Since $I \in S$, we have that $S \neq \emptyset$. It is easy to see that $(S, \subseteq)$ is a poset. Let C be a nonempty chain in S. We claim that

$$U = \bigcup_{J \in C} J$$

is an ideal in R. Since $C \neq \emptyset$, we have that $U \neq \emptyset$. Let $a, b \in U$ and $r \in R$. Then there exist $J_1, J_2 \in C$ such that $a \in J_1$, $b \in J_2$. Since C is a chain, one of $J_1 \subseteq J_2$ and $J_2 \subseteq J_1$ holds. Without loss of generality we assume that $J_1 \subseteq J_2$. Then $a, b \in J_2$ and so

- $a - b \in J_2 \subseteq U \Rightarrow a - b \in U$, and
- $ar, ra \in J_2 \subseteq U \Rightarrow ar, ra \in U$.

Hence U is an ideal in R. Since $I \subseteq J$ for all $J \in C$, we have $I \subseteq U$. Since $1 \notin J$ for all $J \in C$, we have $1 \notin U$ and so $U \neq R$. Hence $U \in S$ is an upper bound of C. By Zorn's lemma there exists a maximal element $M \in S$. Since $I \subseteq M$, it is enough to show that M is a maximal ideal. Assume $M \subseteq N$ for some ideal N of R with $N \neq R$. Then $I \subseteq M \subseteq N$ implies $N \in S$ and so $M = N$ since M is a maximal element. Therefore M is a maximal ideal of R. $\square$