Let $\mathfrak{a} \subset A$ be an ideal in a ring, and $\phi\colon A \to A/\mathfrak{a}$ the quotient homomorphism.

Theorem. *There is a bijective correspondence*

$$\{\textit{Ideals of } A/\mathfrak{a}\} \leftrightarrow \{\textit{Ideals of } A \textit{ containing } \mathfrak{a}\},$$

where the rightward map is

$$\mathfrak{b} \subseteq A/\mathfrak{a} \mapsto \phi^{-1}(\mathfrak{b}) \subseteq A$$

and the leftward map is

$$\mathfrak{a} \subseteq \mathfrak{b} \subset A \mapsto \phi(\mathfrak{b}) = \mathfrak{a}/\mathfrak{b} \subseteq A/\mathfrak{b}$$

Sketch proof. First show ϕ^{-1} is well-defined, i.e. that if $\mathfrak{b} \subseteq A/\mathfrak{a}$ is an ideal, then $\phi^{-1}(\mathfrak{b})$ is an ideal containing $\mathfrak{a}$. Then show ϕ is well-defined, i.e. that if $\mathfrak{b} \subseteq A$ is an ideal containing $\mathfrak{a}$, then $\phi(\mathfrak{b}) \subseteq A/\mathfrak{a}$ is an ideal of $A/\mathfrak{a}$. Finally show that $\phi(\phi^{-1}(\mathfrak{b})) = \mathfrak{b}$ for all ideals $\mathfrak{b} \subseteq A/\mathfrak{a}$ and $\phi^{-1}(\phi(\mathfrak{b})) = \mathfrak{b}$ for all ideals $\mathfrak{b} \subseteq A$ containing $\mathfrak{a}$, so that ϕ and ϕ^{-1} are inverse operations. □

Example. Recall the ideals of $\mathbb{Z}$ are all principal, i.e. of the form (n) for some $n \in \mathbb{Z}$. We have

$$(m) \subseteq (n) \Leftrightarrow m \in (n) \Leftrightarrow m = nk \text{ for some } k \in \mathbb{Z}.$$

Thus the ideals of $\mathbb{Z}/(n)$ are all of the form $(m)/(n)$ for m dividing n.

2. Prime and maximal ideals, special rings

Definition. Let A be a ring.

- An element $x \in A$ is a **unit** if there exists a $y \in A$ such that $xy = 1$.
- An element $0 \neq x \in A$ is a **zero-divisor** if there exists a $y \neq 0$ such that $xy = 0$.
- A ring A is an **integral domain** if $A \neq 0$ and A has no zero-divisors.
- A ring A is a **field** if $A \neq 0$ and every non-zero element is a unit.

Example. The ring $\mathbb{Z}$ is an integral domain since for $x, y \in \mathbb{Z}$, we have $xy = 0 \Rightarrow x = 0$ or $y = 0$. The units of $\mathbb{Z}$ are 1 and -1, so $\mathbb{Z}$ is not a field (e.g. 2 does not have a multiplicative inverse).

The rings $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields, e.g. for every $m/n \in \mathbb{Q} \setminus \{0\}$, we have an inverse element n/m.

The ring $\mathbb{Z}/(4)$ is not an integral domain. We have $2 \neq 0$, but $2 \cdot 2 = 4 = 0$ in $\mathbb{Z}/(4)$, so 2 is a zero-divisor.

Proposition. *Let $x \in A$. Then x is a unit $\Leftrightarrow (x) = (1) = A$.*

Proof. If x is a unit, there exists a $y \in A$ such that $xy = 1$, hence for every $z \in A$, we have $(zy)x = z(yx) = z1 = z \in (x)$, so $(x) = A$.

Conversely, if $(x) = (1)$, then $1 \in (x)$, so there exists a y such that $xy = 1$. □

Theorem. *Let A be a ring. The following are equivalent:*

1. *A is a field.*
2. *A has exactly two ideals, $(0) \neq (1)$.*

Proof. (1) ⇒ (2): Let A be a field, let $\mathfrak{a}$ be an ideal with $\mathfrak{a} \neq (0)$. Then there exists an $x \neq 0$ in $\mathfrak{a}$. Since A is a field, x is a unit, and then by the previous proposition, $(x) = (1)$. As $(1) = (x) \subseteq \mathfrak{a}$, we have $\mathfrak{a} = (1)$.

(2) ⇒ (1): Let x be a non-zero element of A. Then $(x) \neq (0)$, so by our assumption on A we have $(x) = (1)$. By the previous proposition, x is a unit, and since this is true for every non-zero element x, A is a field.

□

2.1. **Prime and maximal ideals.**

Definition. Let A be a ring, and let $\mathfrak{a} \subseteq A$ be an ideal. We say $\mathfrak{a}$ is a

- **prime** ideal if $\mathfrak{a} \neq (1)$, and for any $a, b \in A$ with $a, b \notin \mathfrak{a}$, we have $ab \notin \mathfrak{a}$
- **maximal** ideal if $\mathfrak{a} \neq (1)$, and the only ideal containing $\mathfrak{a}$ is (1).

We write $\mathrm{Spec}(A)$ for the set of prime ideals of A, called the **spectrum** of A.

Example. In $\mathbb{Z}$, the prime ideals are (0) and (p) for primes p. These are prime since

$$a, b \notin (0) \Leftrightarrow a, b \neq 0 \Rightarrow ab \neq 0 \Leftrightarrow ab \notin (0)$$

and

$$a, b \notin (p) \Leftrightarrow p \text{ does not divide } a, b \Rightarrow p \text{ does not divide } ab \Leftrightarrow ab \notin (p)$$

The maximal ideals are the ideals of the form (p) where p is a prime.

Example. Let k be a field. The ideals of $k[x]$ are all principal. An ideal $(f) \subseteq k[x]$ is

- prime if f is irreducible[1] or $f = 0$.
- maximal if f is irreducible.

Proposition. *Let $\mathfrak{a} \subseteq A$ be an ideal. Then $\mathfrak{a}$ is*

(1) *prime if and only if $A/\mathfrak{a}$ is an integral domain.*
(2) *maximal if and only if $A/\mathfrak{a}$ is a field.*

Proof. (1) If $\mathfrak{a}$ is prime, then given $a, b \in A \setminus \mathfrak{a}$, we have $ab \notin \mathfrak{a}$. Then $(a + \mathfrak{a})(b + \mathfrak{a}) = ab + \mathfrak{a} \neq 0 + \mathfrak{a} \in A/\mathfrak{a}$. Conversely, if $\mathfrak{a}$ is not prime, there exist $a, b \in A \setminus \mathfrak{a}$ such that $ab \in \mathfrak{a}$, which gives that $(a + \mathfrak{a})(b + \mathfrak{a}) = 0$ in $A/\mathfrak{a}$, proving $A/\mathfrak{a}$ is not an integral domain.

(2) $A/\mathfrak{a}$ is a field ⇔ $A/\mathfrak{a}$ has exactly two ideals ⇔ There are exactly two ideals in A containing $\mathfrak{a}$ ⇔ $\mathfrak{a}$ is maximal.

□

Corollary. *Let $\mathfrak{a} \subseteq \mathfrak{b} \subseteq A$ be ideals. Then $\mathfrak{b}$ is a prime (resp. maximal) ideal of A if and only if $\mathfrak{b}/\mathfrak{a}$ is a prime (resp. maximal) ideal of $A/\mathfrak{a}$.*

Proof. We have a ring isomorphism $A/\mathfrak{b} \cong (A/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a})$, each side of which is an integral domain (resp. a field) if and only if the other is. □

Corollary. *Every maximal ideal is a prime ideal.*

Proof. $\mathfrak{a}$ maximal ⇔ $A/\mathfrak{a}$ a field ⇒ $A/\mathfrak{a}$ an integral domain ⇔ $\mathfrak{a}$ a prime ideal. □

[1]Recall f is irreducible if there is no way to write $f = gh$ with g and h non-units.

Example. Let k be a field, let $a_1, \ldots, a_n \in k$ and consider the homomorphism $\phi\colon k[x_1, \ldots, x_n] \to k$ given by $\phi(f) = f(a_1, \cdots, a_n)$, i.e. evaluate the polynomial f by substituting a_i for x_i. This ϕ is surjective, and the ideal $\ker \phi$ is maximal, since

$$k[x_1, \ldots, x_n]/\ker \phi \cong \operatorname{im} \phi = k,$$

which is a field.

2.2. **Existence of maximal ideals.**

Theorem 2.1. *Let A be a non-zero ring. There exists a maximal ideal $\mathfrak{m} \subseteq A$.*

Corollary. *If $\mathfrak{a} \subset A$ is an ideal and $\mathfrak{a} \neq (1)$, then there is a maximal ideal $\mathfrak{m}$ containing $\mathfrak{a}$.*

Proof. $A/\mathfrak{a}$ has a maximal ideal $\mathfrak{m}$. With the quotient homomorphism $\phi\colon A \to A/\mathfrak{a}$, we have that $\phi^{-1}(\mathfrak{m})$ is a maximal ideal of A containing $\mathfrak{a}$. □

Corollary. *Let f be a ring. Then f is a non-unit if and only if f is contained in a maximal ideal.*

Proof. f a non-unit $\Leftrightarrow$ $(f) \neq (1) \Leftrightarrow (f) \subseteq \mathfrak{m}$ for a maximal $\mathfrak{m} \Leftrightarrow f \in \mathfrak{m}$ for a maximal $\mathfrak{m}$. □

The proof of the theorem uses **Zorn's lemma**.

Definition. A **partially ordered set** is a set S and a binary relation $\leq$ on the elements of S such that

(1) For all $x \in S$, $x \leq x$.
(2) For $x, y, z \in S$ such that $x \leq y$ and $y \leq z$, we have $x \leq z$.
(3) If $x \leq y$ and $y \leq x$, then $x = y$.

Remark. Given x, y in a partially ordered set S, they may be incomparable in the sense that neither $x \leq y$ nor $y \leq x$.

Definition. Let R be a subset of a partially ordered set $(S, \leq)$. An element $x \in S$ is an **upper bound** for R if for every $y \in R$ we have $y \leq x$.

Definition. An element $x \in S$ is **maximal** if there is no $y \in S$ with $x < y$ (meaning $x \leq y$ and $y \neq x$).

Definition. A subset $R \subseteq S$ of a partially ordered set is a **chain** if for every $x, y \in R$ we have either $x \leq y$ or $y \leq x$.

Example. Let A be a ring, and let S be the set of all its ideals, with the partial ordering given by

$$\mathfrak{a} \leq \mathfrak{b} \Leftrightarrow \mathfrak{a} \subseteq \mathfrak{b}$$

Theorem (Zorn's lemma)**.** *Let S be a partially ordered set, and assume that every chain $R \subseteq S$ has an upper bound. Then S has a maximal element.*

Proof of Theorem 2.1. Let S be the set of ideals $\mathfrak{a} \subseteq A$ such that $\mathfrak{a} \neq (1)$. We claim that every chain in S admits an upper bound. Let $\{\mathfrak{a}_i\}_{i \in R}$ be a chain of ideals in S. Define $\mathfrak{a} = \bigcup_{i \in R} \mathfrak{a}_i$. We then have

(1) $\mathfrak{a}$ is an ideal of A: If $a, b \in \mathfrak{a}$, there are $i, j \in R$ such that $a \in \mathfrak{a}_i$ and $b \in \mathfrak{a}_j$. As R is totally ordered, we have either $\mathfrak{a}_i \subseteq \mathfrak{a}_j$ or $\mathfrak{a}_j \subseteq \mathfrak{a}_i$. Assuming without loss of generality that $\mathfrak{a}_i \subseteq \mathfrak{a}_j$, we have It is easy to check that $\mathfrak{a}$ is closed under taking additive inverses and multiplication from A, so $\mathfrak{a}$ is an ideal.

(2) $\mathfrak{a} \neq (1)$. This is true since if $1 \in \mathfrak{a}$, we must have $1 \in \mathfrak{a}_i$ for some $i \in R$, contradicting the assumption that $\mathfrak{a}_i \in S$.

Thus $\mathfrak{a}$ is an upper bound for the chain R. Since every chain of ideals has an upper bound, Zorn's lemma tells us that maximal ideals exist. $\square$

Remark. Note that it is *not* true in general that a union of ideals is an ideal; e.g. in $\mathbb{Z}$, the set $(2) \cup (3)$ not closed under addition, so is not an ideal.