Definition 19.1

Let R be a ring. An *(both sided) ideal* of R is a subring $I \subseteq R$ such that for any $a \in I$ and $r \in R$ we have $ra \in I$ and $ar \in I$.

We write $I \triangleleft R$ to denote that I is an ideal of R.

Example. For $n \geq 1$ let $n\mathbb{Z}$ denote the set of integers that are multiples of n:

$$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$$

Then $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

In general, if R is a commutative ring and $a \in R$ then define

$$aR = \{ar \mid r \in R\}$$

Ideals of this form are called *principal ideals*.

Example. Let I, J be ideals of a ring R. Define

$$I + J = \{a + b \mid a \in I,\ b \in J\}$$

Then $I + J$ is an ideal of R. Notice that $I, J \subseteq I + J$.

If R is a commutative ring and $a_1, a_2, \ldots, a_n \in R$ then denote:

$$\langle a_1, a_2, \ldots a_n \rangle = a_1R + a_2R + \ldots + a_nR$$

We say that $\langle a_1, a_2, \ldots a_n \rangle$ is the ideal *generated by the elements* $a_1, a_2, \ldots a_n$. This ideal consists of all elements of R of the form

$$a_1r_1 + a_2r_2 + \ldots + a_nr_n$$

for any $r_1, r_2, \ldots, r_n \in R$. This is the smallest ideal of R containing $a_1, a_2, \ldots, a_n$.

Example. The ring $\mathbb{Z}$ is a subring of $\mathbb{Q}$, but it is not an ideal of $\mathbb{Q}$.

Example. Let $R[x]$ be the ring of polynomials with coefficients on a ring R. Define

$$I = \{0 + a_1x + \ldots + a_nx^n \mid a_i \in R,\ n \geq 0\}$$

Then I is an ideal of $R[x]$. Notice that this ideal is a principal ideal: $I = xR[x]$.

Example. In any ring R the smallest ideal is the ideal $\{0\}$, and the largest ideal is R.

Example If R is a ring with unity and $I \triangleleft R$ is an ideal such that $1 \in I$ then $I = R$. Indeed, for any $a \in R$ we have $a = a \cdot 1 \in I$.

Example. If F is a field and $I \triangleleft F$ then either $I = \{0\}$ or $I = F$. Indeed, assume that there is some $a \neq 0$ such that $a \in I$. Then for any $b \in F$ we have $b = (ba^{-1})a$ and so $b \in I$.

Note. Let R be a ring and S be a subring. Since R, taken with addition is an abelian group and S is its normal subgroup, we can consider its quotient group R/S. The elements of R/S are left cosets $a + S$ for $a \in R$ and addition is given by $(a + S) + (b + S) = (a + b) + S$.

Theorem 19.2

Let R be a rings and $I \triangleleft R$. Let $a_1, a_2, b_1, b_2 \in R$ be elements such that $a_1 + I = a_2 + I$ and $b_1 + I = b_2 + I$. Then $(a_1b_1) + I = (a_2b_2) + I$.

Note. Theorem 19.2 is not true if I is a subring of R which is not an ideal. Take for example $R = \mathbb{Q}$ and $I = \mathbb{Z}$. Let $a_1 = \frac{1}{2}$, $a_2 = \frac{1}{2}$, $b_2 = 0$, $b_2 = 1$. We have $a_1 + \mathbb{Z} = a_2 + \mathbb{Z}$ and $b_1 + \mathbb{Z} = b_2 + \mathbb{Z}$. However, $a_1b_1 + \mathbb{Z} = 0 + \mathbb{Z}$ and $a_2b_2 = \frac{1}{2} + \mathbb{Z}$, so $a_1b_1 + \mathbb{Z} \neq a_2b_2 + \mathbb{Z}$.

Proof of Theorem 19.2. If $a_1 + I = a_2 + I$ then $a_2 = a_1 + r$ for some $r \in I$. Similarly, $b_2 = b_1 + r'$ for some $r' \in R$ This gives

$$a_2b_2 = (a_1 + r)(a_2 + r') = a_1a_2 + a_1r' + ra_2 + rr'$$

Since I is an ideal, thus $a_1r' + ra_2 + rr' \in I$, and so $a_2b_2 + I = a_1b_1 + I$. □

Definition 19.3

Let R be a ring and let $I \triangleleft R$. The *quotient ring* R/I is the ring defined as follows:

- Elements of R/I are cosets $a + I$ for $a \in R$.
- Addition: $(a + I) + (b + I) = (a + b) + I$.
- Multiplication: $(a + I) \cdot (b + I) = (ab) + I$.

Note. Let R be a ring and $I \triangleleft R$. If R is commutative then the quotient ring R/I is commutative. If R is a ring with unity $1 \in R$ then R/I is a ring with unity $(1 + I) \in R/I$.

Definition 19.4

Let R be a commutative ring with unity. A *prime ideal* of R is an ideal $I \triangleleft R$ such that $I \neq R$ and if $ab \in I$ then either $a \in I$ or $b \in I$.

Example. Take the ring of integers $\mathbb{Z}$. Recall that

$$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$$

If p is a prime number, then $p\mathbb{Z}$ is a prime ideal. Indeed, if $ab \in p\mathbb{Z}$ then $ab = pk$ for some $k \in \mathbb{Z}$. This means that p divides ab, and so it must divide either a (in which case $a \in p\mathbb{Z}$) or b (and then $b \in p\mathbb{Z}$).

On the other if $n > 0$ is not a prime, then $n = km$ for some $0 < k, m < n$. This gives $k \notin nZ$, $m \notin n\mathbb{Z}$ but $km = n \in n\mathbb{Z}$, so $n\mathbb{Z}$ is not a prime ideal.

Example. The zero ideal $\{0\} \triangleleft R$ is prime if and only if R is an integral domain. Indeed, if $\{0\}$ is not prime if and only if there are non-zero elements $a, b \in R$ such that $ab = 0$.

Theorem 19.5

If R is a commutative ring with unity and $I \triangleleft R$ then I is a prime ideal if and only if R/I in an integral domain.

Proof. Assume that R/I is not an integral domain. Then there are $a, b \in R$ such that $a + I \neq 0 + I$ and $b + I \neq 0 + I$ but $ab + I = 0 + I$. This means that $a \notin I$, $b \notin I$ but $ab \in I$, which shows that I is not a prime ideal.

The proof of the converse is similar. □

Definition 19.6

Let R be a commutative ring with unity. A *maximal ideal* of R is an ideal $I \triangleleft R$ such that $I \neq R$ if $J \triangleleft R$ is any other ideal such that and $I \subseteq J$ and $I \neq J$ then $J = R$.

Example. The ideal $4\mathbb{Z} \triangleleft \mathbb{Z}$ is not maximal since $4\mathbb{Z} \subseteq 2\mathbb{Z}$.

Example. Take the ring $\mathbb{Z}$. We will show that if p is a prime then $p\mathbb{Z}$ is a maximal ideal. Indeed, assume that there is some ideal $J \triangleleft \mathbb{Z}$ such that $p\mathbb{Z} \subseteq J$. Let $a \in J$ and $a \notin p\mathbb{Z}$. Then a is not divisible by p, so $\gcd(p, a) = 1$. As a consequence we can find $k, l \in \mathbb{Z}$ such that $pk + al = 1$. Since $p, a \in J$, this gives $1 \in J$, and so $J = \mathbb{Z}$.

Theorem 19.7

If R is a commutative ring with unity and $I \triangleleft R$ then I is a maximal ideal if and only if R/I in a field.

Proof. Assume that R/I is a field and let $J \triangleleft R$ be an ideal such that $I \subseteq J$ but $I \neq J$. We will show that $J = R$. Indeed, take $a \in J$ such that $a \notin I$. Then $a + I$ is a non-zero element in R/I, so it is a unit in R/I. In other words, there is $b \in R$ such that $(ab + I) = (a + I)(b + I) = 1 + I$. This means that $1 = ab + c$ for some $c \in I$. Since $a \in J$ and $c \in J$ we obtain that $1 \in J$, and so $J = R$.

Conversely, assume that I is a maximal ideal and let $a + I \in R/I$ be a non-zero element. Take $J = I + aR$. Then $I \subseteq J$ and $I \neq J$ since $a \notin I$. By maximality of I we obtain that $J = R$. This means that $1 \in J$, so $1 = c + ab$ for some $c \in I$ and $b \in R$. This gives:

$$1 + I = ab + I = (a + I)(b + I)$$

so $a + I$ is a unit in R/I with $(a + I)^{-1} = b + I$. □

Theorem 19.8

If R is a commutative ring with unity then every maximal ideal of R is a prime ideal.

Proof. If $I \triangleleft R$ is a maximal ideal then R/I is a field by Theorem 19.7, and so by Theorem 18.6 it is an integral domain. Then, Theorem 19.5 implies that I is a prime ideal. □

Example. In the ring $\mathbb{Z}[x]$ define

$$I = \{p(x) \in \mathbb{Z}[x] \mid p(0) = 0\}$$

This is an ideal of $\mathbb{Z}[x]$. We claim that I is a prime ideal. Indeed, if $p(x), q(x) \in I$ are polynomials such that $p(x)q(x) \in I$, then $p(0) \cdot q(0) = 0$, so either $p(0) = 0$ or $q(0) = 0$. This means that either $p(x) \in I$ or $q(x) \in I$.

On the other hand, I is not a maximal ideal. Take, for example

$$J = \{p(x) \in \mathbb{Z}[x] \mid p(0) \text{ is an even number}\}$$

One can check that J is an ideal of $\mathbb{Z}[x]$. We have $I \subseteq J$, but $J \neq \mathbb{Z}[x]$, since e.g. $p(x) = 1 + x \notin J$.