Maximal and Prime Ideals

If R is a ring and N is an ideal in R then R/N is also a ring (a factor ring). The question is under what conditions on R and N will R/N have special features (for example, be an integral domain or a field)?

Ex. If $R = \mathbb{Z}$, an integral domain, and $N = p\mathbb{Z}$, for a prime p, then the factor ring $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$ which is a field.

Ex. The ring $\mathbb{Z} \times \mathbb{Z}$ is not an integral domain because if $a, b \in \mathbb{Z}$, and nonzero

$$(0, a), (b, 0) \in \mathbb{Z} \times \mathbb{Z} \text{ but } (0, a)(b, 0) = (0, 0),$$

However, let $N = \{(n, 0) |\, n \in \mathbb{Z}\}$. N is an ideal in $\mathbb{Z} \times \mathbb{Z}$ because for any $(a, b) \in \mathbb{Z} \times \mathbb{Z}$

$$(a, b)(n, 0) = (an, 0) \in N$$

$$\text{and} \quad (n, 0)(a, b) = (na, 0) \in N.$$

Then $(\mathbb{Z} \times \mathbb{Z})/N$ is isomorphic to $\mathbb{Z}$ under the map:

$$(0, k) + N \to k, \;\; k \in \mathbb{Z}.$$

Thus the factor ring of a ring can be an integral domain even if the original ring is not.

Ex. $N = \{0, 5\} \subseteq \mathbb{Z}_{10}$ is an ideal of $\mathbb{Z}_{10}$, and $\mathbb{Z}_{10}/N$ has 5 elements:

$$0 + N, \;\; 1 + N, \;\; 2 + N, \;\; 3 + N, \;\; 4 + N.$$

$\mathbb{Z}_{10}/N \cong \mathbb{Z}_5$ under the map:

$$k + N \leftrightarrow k.$$

Thus if R is not even an integral domain it's still possible for R/N to be a field.

Ex. $\mathbb{Z}$ is an integral domain but $\mathbb{Z}/8\mathbb{Z} \cong \mathbb{Z}_8$ is not.

Thus, a factor ring may have a stronger structure than the original ring (like the example $\mathbb{Z}_{10}/N \cong \mathbb{Z}_5$) or a weaker structure than the original ring (like $\mathbb{Z}/8\mathbb{Z} \cong \mathbb{Z}_8$).

Def. Every non-zero ring R has at least two ideals. The entire ring R is an ideal, called the **improper ideal** of R. And $\{0\}$ is an ideal of R called the **trivial ideal** of R. A **proper, nontrivial ideal** of a ring R is an ideal N of R such that $N \neq R$ and $N \neq \{0\}$.

Theorem: If R is a ring with unity and N is an ideal of R containing a unit, then $N = R$.

Proof: Let N be an ideal of R, and suppose that $u \in N$ a unit in R.

Thus the condition $aN \subseteq N$ for all $a \in R$ implies that $u^{-1}N \subseteq N$.

Since $u \in N \Longrightarrow u^{-1}(u) = 1 \in N$.

But then $aN \subseteq N \Longrightarrow a(1) \subseteq N$ for all $a \in R$.

Thus $N = R$.

Corollary: A field contains no proper nontrivial ideals.

Proof: Since every non-zero element of a field is a unit, any nontrivial ideal of a field contains a unit and must equal the field.

Def. A **maximal ideal** of a ring R is an ideal M different from R such that there is no proper ideal N of R properly containing M.

Ex. Let $R = \mathbb{Z}$. Then $p\mathbb{Z}, p$ a prime number, is an ideal and a maximal ideal.

$$p\mathbb{Z} = \{\dots, -3p, -2p, -p, 0, p, 2p, 3p, \dots\}.$$

$N = 6\mathbb{Z} = \{\dots, -18, -12, -6, 0, 6, 12, 18, \dots\}$ is an ideal of $\mathbb{Z}$ but it is not maximal as both the ideals,

$$N_1 = 2\mathbb{Z} = \{\dots, -8, -6, -4, -2, 0, 2, 4, 6, 8, \dots\}$$

$$N_2 = 3\mathbb{Z} = \{\dots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \dots\}$$

have the property that $N \subsetneq N_1$ and $N \subsetneq N_2$. Thus N is not a maximal ideal.

Theorem: Let R be a commutative ring with unity. Then M is a maximal ideal of R if, and only if, R/M is a field.

Corollary: A commutative ring with unity is a field if, and only if, it has no proper nontrivial ideals.

Proof: A field has no proper nontrivial ideals. If a commutative ring with unity has no nontrivial ideals, then $\{0\}$ is a maximal ideal and $R/\{0\}$, which is isomorphic to R, is a field by the previous theorem.

If R is a commutative ring with unity when is R/N an integral domain?

R/N is an integral domain if it doesn't have any zero divisors:

if $(a+N)(b+N)=N$ then either

$a+N=N$ or $b+N=N$.

This amounts to saying if $ab\in N$ then either $a\in N$ or $b\in N$.

Def. An ideal $N\neq R$ in a commutative ring R is a **prime ideal** if $ab\in N$ implies that either $a\in N$ or $b\in N$.

$\{0\}$ is always a prime ideal in an integral domain.

Ex. All ideals of $\mathbb{Z}$ are of the form $n\mathbb{Z}$.

$n=0$ gives $n\mathbb{Z}=\{0\}$ and $\mathbb{Z}/n\mathbb{Z}\cong\mathbb{Z}_n$.

If $n=p$ a prime number then $\mathbb{Z}/n\mathbb{Z}=\mathbb{Z}/p\mathbb{Z}\cong\mathbb{Z}_p$ which is an integral domain (in fact, it's a field).

If $n=rs,$ where neither r nor s is 1, then $\mathbb{Z}/n\mathbb{Z}\cong\mathbb{Z}_{rs}$ is not an integral domain as $(r)(s)\equiv 0\ (mod\ rs)$.

So $\mathbb{Z}/n\mathbb{Z}$ is an integral domain when $n=p$, a prime, or $n=0$.

$p\mathbb{Z}$, p a prime, and $\{0\}$ are prime ideals in $\mathbb{Z}$.

So $\mathbb{Z}/n\mathbb{Z}$ is an integral domain when $n\mathbb{Z}$ is a prime ideal.

Theorem: Let R be a commutative ring with unity and let $N \neq R$ be an ideal in R. Then R/N is an integral domain if, and only if, N is a prime ideal.

Corollary: Every maximal ideal in a commutative ring R with unity is a prime ideal.

Proof: If M is maximal in R, then R/M is a field and hence an integral domain and therefore M is a prime ideal.

Ex. Show that $\{0\} \times \mathbb{Z}$ is a prime ideal of $\mathbb{Z} \times \mathbb{Z}$, but not a maximal ideal.

If $(a, b)(c, d) \in \{0\} \times \mathbb{Z}$ then $ac = 0$ in $\mathbb{Z}$.

This implies either $a = 0$ or $c = 0$.

Thus (a, b) or $(c, d) \in \{0\} \times \mathbb{Z}$.

So $\{0\} \times \mathbb{Z}$ is prime.

Notice that $(\mathbb{Z} \times \mathbb{Z})/(\{0\} \times \mathbb{Z}\ ) \cong \mathbb{Z}$ which is an integral domain.

$\{0\} \times \mathbb{Z} \subsetneq n\mathbb{Z} \times \mathbb{Z},\ n \neq 0, 1,$ so $\{0\} \times \mathbb{Z}$ is not maximal.

Ex. Find all prime ideals in $\mathbb{Z}_6$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$.

The ideals in $\mathbb{Z}_6$ are:

$$\mathbb{Z}_6, \;\; 2\mathbb{Z}_6 = \{0, 2, 4\}, \;\; 3\mathbb{Z}_6 = \{0,3\}, \text{ and } \{0\}.$$

$\{0\}$ is not a prime ideal because $(2)(3) \equiv 0 \; (mod 6)$

If $ab \in 2\mathbb{Z}_6 = \{0, 2, 4\}$, then either a or b is in $2\mathbb{Z}_6$ so $2\mathbb{Z}_6$ is prime.

If $ab \in 3\mathbb{Z}_6 = \{0, 3\}$, then either a or b must be a multiple of 3 so a or b is in $3\mathbb{Z}_6$. So $3\mathbb{Z}_6$ is prime.

By definition a prime ideal $\neq R$ so $\mathbb{Z}_6$ is not a prime ideal in $\mathbb{Z}_6$.

So $2\mathbb{Z}_6, 3\mathbb{Z}_6$ are the prime ideals in $\mathbb{Z}_6$.

The ideals in $\mathbb{Z}_2 \times \mathbb{Z}_2$ are:

$$\mathbb{Z}_2 \times \mathbb{Z}_2, \;\; \{0\} \times \mathbb{Z}_2, \;\; \mathbb{Z}_2 \times \{0\}, \text{ and } \{0\} \times \{0\}.$$

If $(a, b)(c, d) \in \{0\} \times \mathbb{Z}_2$, then $ac = 0$ thus either $a = 0$, which means $(a, b) \in \{0\} \times \mathbb{Z}_2$ or $c = 0$, which means $(c, d) \in \{0\} \times \mathbb{Z}_2$. Thus $\{0\} \times \mathbb{Z}_2$ is prime.

A similar argument shows that $\mathbb{Z}_2 \times \{0\}$ is prime.

$\{0\} \times \{0\}$ is not prime because $(1,0)(0,1) = (0,0)$.

$\mathbb{Z}_2 \times \mathbb{Z}_2$ cannot be prime in $\mathbb{Z}_2 \times \mathbb{Z}_2$.

So the prime ideals in $\mathbb{Z}_2 \times \mathbb{Z}_2$ are: $\{0\} \times \mathbb{Z}_2 \; and \; \mathbb{Z}_2 \times \{0\}$.

So to summarize, for a commutative ring R with unity:

1) An ideal M of R is maximal if, and only if, R/M is a field.
2) An ideal N of R is prime if, and only if, R/N is an integral domain.
3) Every maximal ideal of R is a prime ideal.

We will not prove this, but every field F contains either a subfield isomorphic to $\mathbb{Z}_p$, for some prime p, or a subfield isomorphic to $\mathbb{Q}$.

Thus $\mathbb{Z}_p$ and $\mathbb{Q}$ are the fundamental building blocks of all fields.

Def. The fields $\mathbb{Z}_p$ and $\mathbb{Q}$ are called **prime fields**.

Def. If R is a commutative ring with unity and $a \in R$, the ideal $\{ra | \, r \in R\}$ of all multiples of a is the **principal ideal generated by a** and is denoted $< a >$. An ideal N of R is a **principal ideal** if $N =< a >$ for some $a \in R$.

Ex. Every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$, which is generated by n, so every ideal of $\mathbb{Z}$ is a principal ideal.

Ex. The ideal $< x >$ in $F[x]$, F a field, consists of all polynomials in $F[x]$ having zero constant term.

Theorem: If F is a field then every ideal in $F[x]$ is principal.

Theorem: An ideal $< p(x) > \neq \{0\}$ of $F[x]$ is maximal if, and only if, $p(x)$ is irreducible over F.

Proof: Suppose $< p(x) >$ is maximal.

If $p(x) = q(x)t(x)$, $q(x), t(x)$ nonconstant polynomials then both are lower degree and $< q(x) > \supsetneq < p(x) >$. So $< p(x) >$ is not maximal, thus $p(x)$ must be irreducible.

Assume $p(x)$ is irreducible over F.

If $< p(x) > \subseteq N \subsetneq F[x]$, then N is a principal ideal by our last theorem. So $N =< t(x) >$ and $p(x) \in N$:

$$p(x) = t(x)r(x).$$

But $p(x)$ is irreducible so $t(x)$ or $r(x)$ is degree 0.
If $t(x)$ is degree 0, then $t(x)$ is a unit and $< t(x) > = F[x]$.
If $r(x)$ is degree 0 then $r(x) = C \in F$ and $t(x) = \frac{1}{c}p(x)$ and

$< t(x) > \subseteq < p(x) >$ so $N = < p(x) >$, so $< p(x) >$ is maximal.

Ex. $x^3 + x + 1$ is irreducible in $\mathbb{Z}_5[x]$ (it has no zeros), so $< x^3 + 3x + 2 >$ is a maximal ideal and $\mathbb{Z}_5[x]/< x^3 + x + 1 >$ is a field.

Ex. $x^2 - 3$ is irreducible in $\mathbb{Q}[x]$, so $\mathbb{Q}[x]/ < (x^2 - 3) >$ is a field.

Ex. Find all c in $\mathbb{Z}_3$ such that $\mathbb{Z}_3[x]/ < (x^3 + cx^2 + 1) >$ is a field.

We need to find all c in $\mathbb{Z}_3$ such that $x^3 + cx^2 + 1$ is irreducible.
Since it's degree 3 we just need to show it has no zero in $\mathbb{Z}_3$. Test c values.

$c = 0$: $x^3 + 1$;

$x = 0$; $0^3 + 1 = 1$;

$x = 1$, $1^3 + 1 = 2$;

$x = 2$; $2^3 + 1 = 2^3 + 1 \equiv 0 \ (mod\ 3)$.

So $x^3 + 1$ does have a zero and is not irreducible in $\mathbb{Z}_3[x]$.

$c = 1$: $x^3 + x^2 + 1$;

$x = 0$; $0^3 + 0^2 + 1 = 1$;

$x = 1$; $1^3 + 1 + 1 \equiv 0 \ (mod\ 3)$.

So it also has a zero and is not irreducible.

$c = 2$: $x^3 + 2x^2 + 1$;

$x = 0$; $0^3 + 2(0^2) + 1 = 1$;

$x = 1$; $1^3 + 2(1^2) + 1 \equiv 1 \ (mod\ 3)$;

$x = 2$, $2^3 + 2(2^2) + 1 \equiv 2 \ (mod\ 3)$.

So $x^3 + 2x^2 + 1$ is irreducible in $\mathbb{Z}_3[x]$.

Thus only for $c = 2$ is $\mathbb{Z}_3[x]/ < (x^3 + cx^2 + 1) >$ a field.

Theorem: Let $p(x)$ be an irreducible polynomial in $F[x]$. If $p(x)$ divides $q(x)t(x)$ for $q(x), t(x) \in F[x]$, then either $p(x)$ divides $q(x)$ or $p(x)$ divides $t(x)$.

Proof: Suppose $p(x)$ divides $q(x)t(x)$.

Then $q(x)t(x) \in < p(x) >$, which is maximal since $p(x)$ is irreducible.

Therefore, $< p(x) >$ is a prime ideal, since every maximal ideal in a commutative ring with unity is prime.

Hence, $q(x)t(x) \in < p(x) >$ implies $q(x) \in < p(x) >$ or $t(x) \in < p(x) >$.

Therefore, $p(x)$ divides $q(x)$ or $p(x)$ divides $t(x)$.