Examples of ideals

Given the ring $R = \mathbb{Z}$, it is easy to prove that $n\cdot\mathbb{Z}$ (multiples of n) is an ideal. Let's see it:

$0 \in I$? $\quad I \ni n\cdot 0 = 0$

Is it closed for the addition? $\quad r,s \in \mathbb{Z} \quad nr + ns = n(r+s) \in I$ because $r+s \in \mathbb{Z}$

(Distributivity of the product over the sum)

Is it closed for the additive inverses? $\quad$ If $n\cdot r \in I$ with $r \in \mathbb{Z}$, we just have to consider $-r \in \mathbb{Z}$ to obtain the opposite of nr.

$R\cdot I \subset I$? $\quad n\cdot r \in I$

If we consider another element $s \in \mathbb{Z}$, we have that $s\cdot n\cdot r = n\cdot sr$ so $n(sr) \in I$

(Commutative ring; $sr \in \mathbb{Z}$)

Given the ring $R = k[x]$ it is easy to prove that fixing a polynomial P in $k[x]$, $M(x)\cdot P(x)$ is an ideal (multiples of $P(x)$)

$0 \in I$? $\quad$ Just taking $M(x) = 0$, $0\cdot P(x) = 0 \in I$

Is it closed for the addition? $\quad M(x), N(x) \in k[x]$

Then, $M(x)P(x) + N(x)P(x) = (M(x)+N(x))P(x) \in I$

(Distributivity of the product over the sum; $M(x)+N(x) \in k[x]$)

Is it closed for the additive inverses? $\quad$ If $M(x)\cdot P(x) \in I$ with $M(x) \in k[x]$, we just have to consider $-M(x) \in k[x]$ to obtain the opposite of $M(x)\cdot P(x)$

$R\cdot I \subset I$? $\quad M(x)\cdot P(x) \in I$

If we consider another element $N(x) \in k[x]$, we have that $N(x)\cdot M(x)\cdot P(x) \in I$ because $N(x)\cdot M(x)$ is still a polynomial in $k[x]$.

Definition: Abstracting the previous 2 examples, we can define the **principal ideal generated by n**: $\langle n \rangle = R\cdot n$ which is the set $I = R\cdot n = \{r\cdot n : r \in R\}$ of multiples of n.

Definition: The trivial ideal is $I = \{0\}$.

Definition: We say that an ideal is a proper ideal if it is neither the trivial ideal ($I = \{0\}$) nor the whole ring R.

After seeing this 3 definitions and linking with the examples above we are going to see two results which are analogues:

Corollary: Every ideal I in $\mathbb{Z}$ is principal, that is, of the form $I = n\cdot\mathbb{Z}$. In particular, unless $I = \{0\}$, the integer n is the least positive element of I.

Corollary: Every ideal I in $k[x]$ is principal, that is, of the form $I = k[x]\,p(x)$ for some polynomial P. In particular, P is the monic polynomial of smallest degree in I, unless $I = \{0\}$ in which case $p(x) = 0$

Proof of the first corollary:

We suppose that $I \neq \{0\}$. Let n be the least element of I. Let $x \in I$, take $q, r \in \mathbb{Z}$ with $0 \leq r < n$ such that $x = qn + r$. We can do this because $\mathbb{Z}$ is an Euclidean ring so there exists the algorithm of division. It is clear that $qn \in I$, and since I is closed under additive inverses, $-qn \in I$ too. Since $r = x - qn$ and $x, qn \in I$, then $r \in I$. $0 \leq r < n$ and n is the smallest positive element in I, so it must be $r = 0$. Thus, $x = qn \in n\mathbb{Z}$. ∎

Remark: Every ideal in a Euclidean ring is principal. The proof is always based on the algorithm of division.

Def.: An ideal $\mathfrak{M}$ in R is a maximal ideal if there is no ideal strictly larger than $\mathfrak{M}$ (containing $\mathfrak{M}$) except R itself.

Proposition: For a commutative ring R with unit, and for an ideal I, the quotient ring R/I is a field if and only if I is a maximal ideal.

(field = cuerpo (every non-zero element is a unit, it has an inverse))

$\Leftarrow$ Let $x+I$ be a non-zero element of R/I and let's see that it has an inverse element in R/I. Given that $x+I \neq 0+I$, then $x \notin I$. Now let's consider the ideal $Rx+I$ (it is an ideal because of the constructions that Andrea has explained before). It is strictly larger than I because it is easy to see that $I \subset Rx+I$. Since I is already maximal, $Rx+I$ must be R, so $Rx+I=R$. This implies that there exists $r \in R$ and $i \in I$ such that $rx+i=1$ (this is because we saw before that if an ideal has the element $1 \in I$, then $I=R$. In this case, $Rx+I=R$, so $1 \in Rx+I$). Looking at $rx+i=1$, we know that $rx-1 \in I$, so $rx \equiv 1 \mod I$. This means that the inverse of $x+I$ is $r+I$ because using the definition of multiplication and that $rx \equiv 1 \mod I$, we have that: $(r+I)(x+I) = (rx)+I = 1+I$ (by def.; $rx \equiv 1 \mod I$)

$\Rightarrow$ We suppose that R/I is a field. Let $x \in R$ but $x \notin I$. Then $x+I \neq 0+I$ in R/I. $x+I$ has a multiplicative inverse $r+I$ in R/I: $(x+I)(r+I) = 1+I$

By definition, we know that this is $rx+I = 1+I$, so $1 \in rx+I$, and this implies that the ideal $Rx+I=R$. At the same time, $Rx+I$ is the smallest ideal that contains x and I, so we can conclude that I is a maximal ideal as there are no other improper ideals that contain I.

Prime ideals and integral domains

Def: Let R be a commutative ring with unit 1. An ideal P in R is prime if $ab \in P$ implies either $a \in P$ or $b \in P$.

Examples:

- $\mathbb{Z}[x] \cdot x$ is a prime ideal. If $a, b \in \mathbb{Z}[x]$ and $ab \in \mathbb{Z}[x] \cdot x$, then the polynomial ab is of the form $c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x$. Imagine that $a, b \notin \mathbb{Z}[x] \cdot x$, so a and b both have an independent term. This would lead us to a contradiction because ab would have an independent term that is equal to the product of the independent terms of a and b. In conclusion, a or b must be a polynomial without independent term $\Rightarrow$ a or $b \in \mathbb{Z}[x] \cdot x$
- $\mathbb{Z}[x] \cdot 2x$ is not a prime ideal. Let's see a counterexample:

$$\underset{\mathbb{Z}[x]\cdot 2x}{(4x+2)}\underset{\mathbb{Z}[x]\cdot 2x}{(3x^2+6x)} = 12x^3 + 30x^2 + 12x \in \mathbb{Z}[x] \cdot 2x$$

Def: An integral domain is a commutative ring in which the product of any two nonzero elements is nonzero ($cd = 0$ $c, d \in R$ then $c = 0$ or $d = 0$).

Proposition. For a commutative ring R with unit, and for an ideal I, the quotient ring R/I is an integral domain if and only if I is a prime ideal.

$\Leftarrow$ Let I be prime. Let's suppose that $(x+I)(y+I) = 0+I$ $(x, y \in R)$ and let's see that x or y are in I ($x+I = 0+I$ or $y+I = 0+I$). This way, we would have that R/I is an integral domain. By definition of the multiplication in R/I, we have that

$(x+I)(y+I) = xy+I = 0+I \Rightarrow xy \in I$. I is prime, so x or y is in I, so either $x+I = 0+I$ or $y+I = 0+I$.

$\Leftarrow$ Let's suppose that R/I is an integral domain. Suppose that $xy \in I$ and see that x or y is in I to conclude that I is a prime ideal. Using the definition of the product in R/I, we have that $(x+I)(y+I) = xy+I = 0+I$ ($xy \in I$). Since R/I is an i.d., either

$x+I = 0+I$ or $y+I = 0+I \Rightarrow x \in I$ or $y \in I \Rightarrow I$ is prime

Corollary: Maximal ideals are prime.

Let's see with an example that this isn't true in the other way:

Worked examples

1. Determine the ideals of the field $\mathbb{R}$ (real numbers).

Let's consider an ideal $I \neq \{0\}$ in $\mathbb{R}$. Since all the elements in $\mathbb{R} \setminus \{0\}$ are units (they have inverses), we consider a unit $u \in \mathbb{R}$ that belongs to I ($u \in I$). Since $u^{-1} \in \mathbb{R}$ and $\mathbb{R} \cdot I \subset I$, $u^{-1} \cdot u = 1 \in I \Rightarrow I = \mathbb{R}$

This means that in any field K, and in particular in $\mathbb{R}$, all ideals are trivial ($I = \{0\}$) or the total ($I = K = \mathbb{R}$)

2. What condition must be met for the ideal $m\mathbb{Z}$ to be contained in $n\mathbb{Z}$?

This is easy to infer from a simple example. Let's consider $6\mathbb{Z} = \{0, 6, 12, 18, \ldots\}$. It is contained in

$2\mathbb{Z} = \{0, 2, 4, 6, 8, 10, \ldots\}$ and $3\mathbb{Z} = \{0, 3, 6, 9, 12, \ldots\}$.

Since $6 = 3 \cdot 2$, we know that all the factors of 6 are factors of 2 and 3. In conclusion, $m\mathbb{Z} \subset n\mathbb{Z}$ when $n \mid m$. Now, we also know that some ideals from $\mathbb{Z}$ are not maximal (in particular, $m\mathbb{Z}$ is not maximal when m is not a prime number (it has divisors which are not 1 or m).