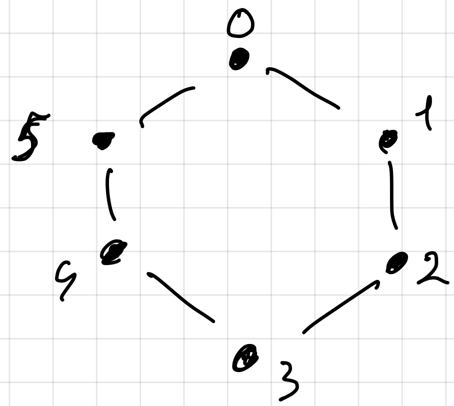
Remark 4.10 $\mathbb{Z}/m\mathbb{Z}$ is a structure obtained out of $\mathbb{Z}$, in which the element m is "declared" to become zero. You can also visualize it as a rotary switch with m positions.



$7 \equiv 1 \mod 6$

$[7]_6 = [1]_6$

One also writes $\mathbb{Z}/m\mathbb{Z}$ as $\mathbb{Z}/m$ or $\mathbb{Z}_m$.

Among rings $\mathbb{Z}/m\mathbb{Z}$, some are fields, some not. We want to understand, which are the fields, because one can do linear algebra over a field and then introduce linear codes.

We will clarify when a general quotient ring R/I is a field.

Def 4.11 In a unitary commutative ring R an ideal I is called maximal if $I \neq R$ and there is no ideal J with $I \subsetneq J \subsetneq R$.

Examples 4.12

- $2\mathbb{Z}$ ideal in $\mathbb{Z}$. Is it maximal?

  Every ideal that contains $2\mathbb{Z}$ and some odd number will be the whole ring ring $\mathbb{Z}$.

  So, $2\mathbb{Z}$ is a maximal ideal.

- $6\mathbb{Z}$ is not maximal, because $6\mathbb{Z} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$

$$\boxed{\begin{array}{c} A \subsetneq B \\ \text{means} \\ A \subseteq B \text{ and } A \neq B. \end{array}}$$

Theorem 4.13 Let R be a unitary commutative ring and I be an ideal in R with $I \neq R$. Then the quotient ring R/I is a field if and only if the ideal I is maximal.

Proof: Assume that I is maximal. Consider an arbitrary non-zero element of R/I, which is the coset $[a]_I$ with $a \notin I$.

Now, consider the smallest ideal that contains I as a subset and the element a, this is

$$I + aR = \{u + a \cdot r : u \in I, r \in R\}.$$

Since I is a maximal ideal, this larger ideal $I + aR$ coincides with the whole ring R.

In particular 1 belongs to $I + aR$. This means

$$1 = u + a \cdot r \quad \text{for some } u \in I \text{ and some } r \in R.$$

$$\Rightarrow \quad a \cdot r \equiv 1 \mod I \quad \Rightarrow \quad [a]_I \cdot [r]_I = [1]_I$$

$\Rightarrow$ $[r]_I$ is the inverse of $[a]_I$,

$$[a]_I^{-1} = [r]_I .$$

Now, assume that the ideal I is not maximal and show that in this case R/I is not a field. Let's pick an ideal J larger than I and smaller than R, that is, $I \subsetneq J \subsetneq R$. Next, pick an element $a \in J$ with $a \notin I$. Then $I + aR$ is an ideal that is larger than I, that contains a and is contained in J. In particular, $I + aR \neq R$. We claim that the coset $[a]_I$ does not have an inverse element.

For, assume the contrary, then $[a]_I \cdot [b]_I$ would be equal to $[1]_I$ for some $b \in R$. This would mean that

$$a \cdot b \equiv 1 \mod I . \Rightarrow$$

$$1 \in a \cdot b + I \subseteq aR + I \Rightarrow$$

$$1 \in I + aR \Rightarrow I + aR = R,$$

which is a contradiction. $\square$

$\boxed{4.3.}$ Ring structure behind the modular arithmetic

We want to know ideals in $\mathbb{Z}$ and see which of them are maximal.

It turns out that in $\mathbb{Z}$, every ideal can be generated by just one element

Example 4.14 $10\mathbb{Z} + 24\mathbb{Z} = m\mathbb{Z}$ for some m.

$$10\mathbb{Z} + 24\mathbb{Z} = 2\mathbb{Z}.$$

$$10\mathbb{Z} + 24\mathbb{Z} \subseteq 2\mathbb{Z}$$

But why the opposite $2\mathbb{Z} \subseteq 10\mathbb{Z} + 24\mathbb{Z}$?

It's about checking if $2 \in 10\mathbb{Z} + 24\mathbb{Z}$?

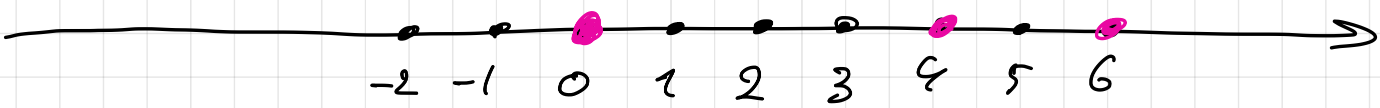
$$50 - 48 = 2$$

$$10 \cdot \underset{\mathbb{Z}}{\underset{\cap}{5}} + 24 \cdot \underset{\mathbb{Z}}{\underset{\cap}{(-2)}} = 2$$

Theorem 4.15. Every ideal in the ring $\mathbb{Z}$ is generated by just one element, that means, it has the form $m\mathbb{Z}$ with $m \in \mathbb{N}_0$.

$$\boxed{\mathbb{N}_0 = \{0, 1, 2, \dots\}}$$

Proof: Let I be an arbitrary ideal. If I has no other elements than zero, then $I = m\mathbb{Z}$ with $m = 0$. Now, assume I has some other elements apart from 0.



Let's pick two elements $a, b \in I$ with $a < b$ such that their difference $b - a$ is minimized. We claim that $I = m\mathbb{Z}$ with $m = b - a$.

Indeed, one has $m\mathbb{Z} \subseteq I$, because for every $z \in \mathbb{Z}$ one has $m \cdot z = (b-a) \cdot z = \underbrace{b \cdot z}_{\overset{\cap}{I}} - \underbrace{a \cdot z}_{\overset{\cap}{I}} \in I$.

We need to check that $m\mathbb{Z} \subseteq I$ is in fact an equality. If we had some $u \in I$ which is not in $m\mathbb{Z}$, then we could do long division of u by m obtaining:

$$u = q \cdot m + r \quad \text{with } q \in \mathbb{Z} \text{ and}$$
$$r \in \{1, \dots, m-1\}.$$

$$\Rightarrow \quad r = \underset{\underset{I}{\cap}}{u} - \underset{\underset{I}{\cap}}{q \cdot m} \in I \quad \text{and the}$$

distance of $r \in I$ to $0 \in I$ is smaller than m, which is a contradiction to the choice of m. This shows $I = m\mathbb{Z}$.

$\square$

So, every nonnegative integer $m \in \mathbb{N}_0$ gives the ideal $m\mathbb{Z}$ in $\mathbb{Z}$. These are all ideals. In order to understand, which of them are maximal, we need to compare them w.r.t. inclusion.

Proposition 4.16 Let $\ell, m \in \mathbb{N}$. Then $\ell\mathbb{Z} \subseteq m\mathbb{Z}$ if and only if ℓ is divisible by m.

Proof: If ℓ is divisible by m then $\frac{\ell}{m} \in \mathbb{Z}$ and one has

$$\ell z = m \cdot \underbrace{\frac{\ell}{m} z}_{\in \mathbb{Z}} \in m\mathbb{Z}$$

for all $z \in \mathbb{Z}$. Conversely, if

$$\ell\mathbb{Z} \subseteq m\mathbb{Z}, \text{ then } \ell \cdot 1 \in m\mathbb{Z},$$

which means that $\ell = m \cdot z$ for some $z \in \mathbb{Z}$

$\Rightarrow$ ℓ is divisible by m.

$\square$

Example 4.17

$$\begin{tikzcd}[column sep=small, row sep=small]
 & 8\mathbb{Z} \arrow[r, phantom, "\subseteq"] & 4\mathbb{Z} \arrow[r, phantom, "\subseteq"] & 2\mathbb{Z} \\
24\mathbb{Z} \arrow[ur, phantom, "\subseteq" sloped] \arrow[dr, phantom, "\subseteq" sloped] & & & \\
 & 12\mathbb{Z} \arrow[r, phantom, "\subseteq"] \arrow[uur, phantom, "\subseteq" sloped] & 6\mathbb{Z} \arrow[r, phantom, "\subseteq"] \arrow[uur, phantom, "\subseteq" sloped] & 3\mathbb{Z}
\end{tikzcd}$$

Theorem 4.18 For $n \in \mathbb{N}$, the ring $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime number.