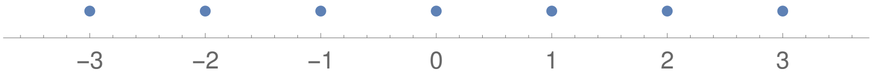
What is...a ring?

Or: Generalizing the integers

A good old friend – the integers $\mathbb{Z}$



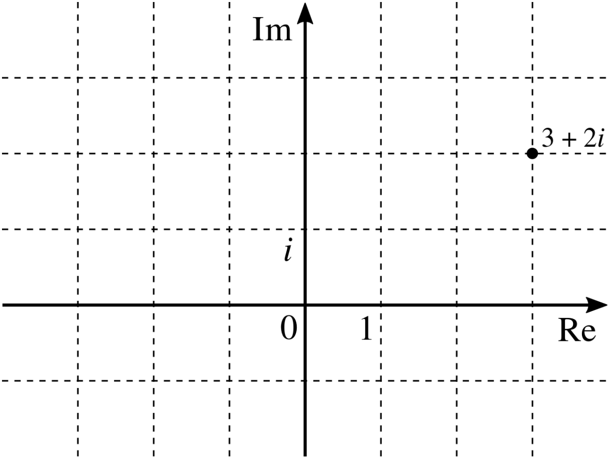
(a) $\mathbb{Z}$ has an addition $+$, $\mathbb{Z}$ has a multiplication $\cdot$ Two operations

(b) $(\mathbb{Z}, +)$ is an abelian group

(c) $(\mathbb{Z}, \cdot)$ is an abelian monoid

(d) The two rules distribute over one another Compatibility

The Gaussian integers $\mathbb{Z}[i]$, $i^2 + 1 = 0$



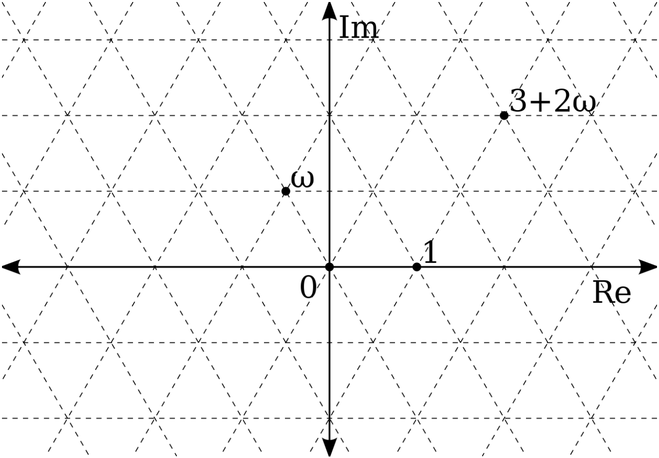
(a) $\mathbb{Z}[i]$ has an addition $+$, $\mathbb{Z}[i]$ has a multiplication $\cdot$ Two operations

(b) $(\mathbb{Z}[i], +)$ is an abelian group

(c) $(\mathbb{Z}[i], \cdot)$ is an abelian monoid

(d) The two rules distribute over one another Compatibility

The Eisenstein integers $\mathbb{Z}[\omega]$, $\omega^2 + \omega + 1 = 0$



(a) $\mathbb{Z}[\omega]$ has an addition $+$, $\mathbb{Z}[\omega]$ has a multiplication $\cdot$ Two operations

(b) $(\mathbb{Z}[\omega], +)$ is an abelian group

(c) $(\mathbb{Z}[\omega], \cdot)$ is an abelian monoid

(d) The two rules distribute over one another Compatibility

For completeness: A formal definition

A commutative ring R is a set such that:

(a) R has an addition $+$, R has a multiplication $\cdot$ Two operations

(b) $(R, +)$ is an abelian group

(c) $(R, \cdot)$ is an abelian monoid

(d) The two rules distribute over one another Compatibility

For a ring one drop the assumption that $ab = ba$
Rings generalize matrices over $\mathbb{Z}$:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Generalizing concepts from $\mathbb{Z}$ to R

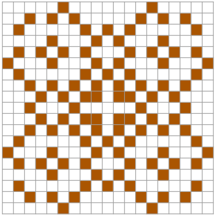
$a \in \mathbb{Z}[i]$ is a Gaussian prime if $a = bc$ implies $b = \pm ia$

- $a + bi$ is a Gaussian prime if and only if $a = p$ or $b = p$ is prime for $p \equiv 3 \bmod 4$, or $a^2 + b^2$ is prime

$$2 = (1+i)(1-i), \quad 5 = (2+i)(2-i)$$

- Every Gaussian integer $a + bi$ can be factor into Gaussian primes

$$10 = 2 \cdot 5 = (1+i)(1-i)(2+i)(2-i)$$



- Such a factorization is unique up to units

Ring theory studies properties of $\mathbb{Z}$ under a more general umbrella

Thank you for your attention!

I hope that was of some help.