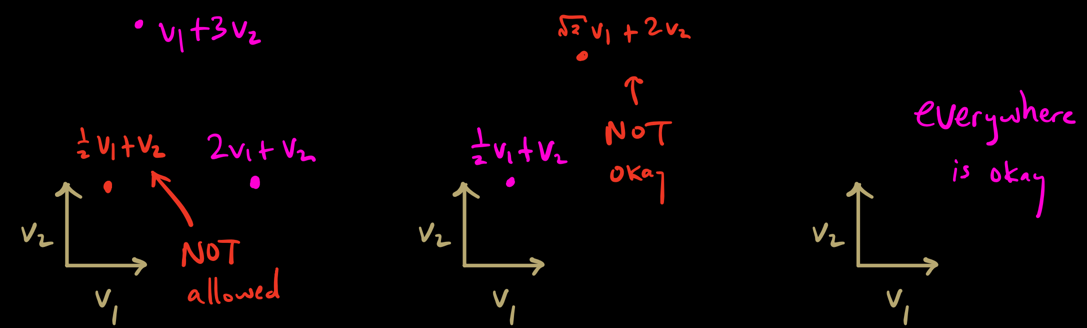
Rings and things

Rings are underlying "number systems"
or "coefficient systems."

Ex. linear combinations of arrows in 2D



$\mathbb{Z}$ $\qquad\qquad$ $\mathbb{Q}$ $\qquad\qquad$ $\mathbb{R}$

Rings generalize the properties of these number systems.

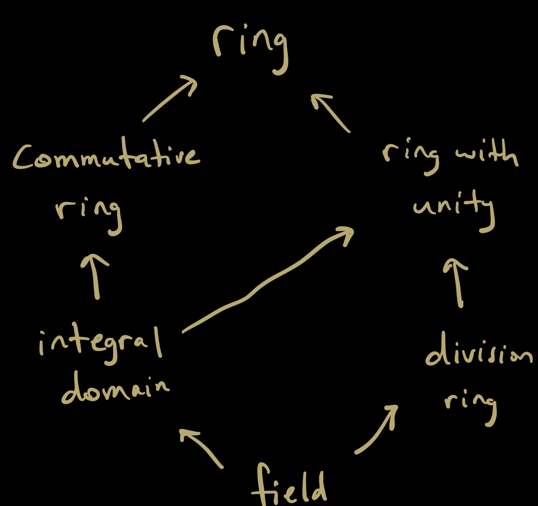
Def. A **ring** is a triple $(R, +, *)$, where R is a nonempty set and $+, *$ are closed binary operations on R satisfying:

1. $a + b = b + a$;
2. $(a+b)+c = a+(b+c)$;
3. $\exists\, 0 \in R$ s.t. $a + 0 = a$, $\forall a \in R$;
4. $\forall a \in R$, $\exists -a \in R$ s.t. $a + (-a) = 0$;
5. $(a*b)*c = a*(b*c)$;
6. distributive laws:
   $a*(b+c) = a*b + a*c$
   $(a+b)*c = a*c + b*c$.

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

Let $(R, +, *)$ be a ring.

- Call R a **ring with unity** (or **ring with identity**) if $\exists\ 1 \neq 0 \in R$ s.t. $1a = a1$, for every $a \in R$.
- Call R a **commutative ring** if $*$ is commutative.
- If $a, b \in R$ are nonzero, but $ab = 0$, then we call a & b **zero divisors.**
- Call R an **integral domain** if it's a commutative ring with no zero divisors.
- A **unit** of a ring with unity is a nonzero elt $a \in R$ for which $\exists!\ a^{-1} \in R$ s.t. $a * a^{-1} = a^{-1} * a = 1$.
- A **division ring** is a ring with unity in which all nonzero elements are units.
- A **field** is a commutative division ring.



Ex

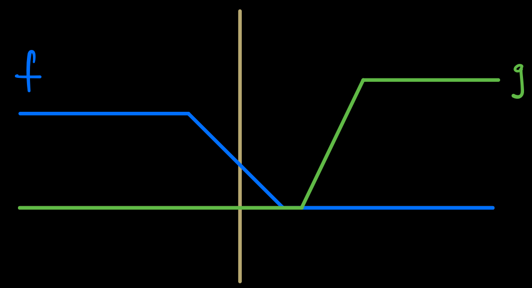
1. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$ are all fields

2. $\mathbb{Z}$ is an integral domain, but not a field
   ($mn=0 \Rightarrow m=0$ or $n=0$) (e.g., $4^{-1} \notin \mathbb{Z}$)

3. $\mathbb{Z}_n$ is a ring, for any $n \geq 1$.
   n prime $\Rightarrow \mathbb{Z}_n$ is a field
   n composite $\Rightarrow \mathbb{Z}_n$ is not an I.D.

4. $C^0(\mathbb{R}) = \{$cts functions $\mathbb{R} \to \mathbb{R}\}$ is a ring under pointwise addition & mult.
   $(f+g)(x) := f(x) + g(x)$ $(fg)(x) := f(x)g(x)$.

   NOT an integral domain



5. $\mathbb{Z}[x] = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \mid a_i \in \mathbb{Z}\}$
   $\llcorner$ n is not fixed

   is an integral domain, not a field
   (no zero divisors) (e.g., $\frac{1}{x} \notin \mathbb{Z}[x]$)

   Similarly, $\mathbb{R}[x]$ is an I.D., not a field.

   R an I.D. $\Rightarrow R[x]$ is an I.D.

⑥ $M_{n\times n}(\mathbb{R})$ is a non-commutative ring with unity.

addition is entry-wise $\qquad 1 = I_n$.

multiplication is matrix multiplication.

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \rightarrow$$ NOT an integral domain.

⑦ The Gaussian integers $\mathbb{Z}[i] := \{m + ni \mid m, n \in \mathbb{Z}\}$ form an I.D., not a field.

Rings & subrings

Prop. Let R be a ring and consider $a, b \in R$. Then

① $a * 0 = 0 * a = 0$;

② $a * (-b) = (-a) * b = -(a * b)$;

③ $(-a) * (-b) = a * b$.

(Proof.) Exercise. ☒

Def. A subring of $(R, +_R, *_R)$ is a ring $(S, +_S, *_S)$ where $S \subseteq R$ and $+_S$ & $*_S$ are restrictions of $+_R$ & $*_S$.

Prop. Let R be a ring and $S \subseteq R$. Then S is a subring of R iff

① $S \neq \phi$;

② $r - s \in S$, $\forall\, r, s \in S$;

③ $rs \in S$, $\forall\, r, s \in S$.

(Proof.) Exercise. ▨

Ex. ① $R = M_{n\times n}(\mathbb{R})$. $GL_n(\mathbb{R})$ is <u>NOT</u> a subring.

$T = \{\text{upper triangular matrices}\}$ is a subring.

② $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ are subrings

Integral domains

Prop. Let D be a commutative ring with identity. Then D is an I.D iff $ab = ac \Rightarrow b = c$, whenever $a \neq 0$.

(Proof). Exercise. ▨

Rmk. We could equivalently state this with right cancellation.

Thm. (Wedderburn)

Every finite integral domain is a field.