Fields

Basic idea:

- In rings, one can add +, substract −, multiply ×
- In "fields" 〃 〃 〃 $\boxed{\text{and}}$ divide.

I] Preliminary: multiplicative inverses in rings.

What are examples of situations in which we can, or cannot, "divide" in a ring? (By divide, here, we mean find the multiplicative inverse of an element).

Ex. 1 $\mathbb{Z}$. 1 and -1 have inverses for $\times$

2 does not (it would be $\frac{1}{2}$, which is not in $\mathbb{Z}$).

Ex. 2 $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2};\ a, b \text{ in } \mathbb{Z}\}$

$1, -1$ still have inverses

$1+\sqrt{2}$ also, indeed $(1+\sqrt{2})(-1+\sqrt{2}) = 2 - 1 = 1$,

So $(1+\sqrt{2})^{-1} = -1+\sqrt{2}$

2 still does not have an inverse ...

Ex. 3 $\mathbb{Z}_4 = \{\underline{0}; \underline{1}; \underline{2}; \underline{3}\}$

Can observe that $\underline{3} \times \underline{3} = \underline{1}$, so $\underline{3}$ has a multiplicative inverse: itself.

However, $\underline{2}$ does not have an inverse, as can be found by checking all possibilities.

Ex. 4 $\mathbb{Z}_{36}$ One can observe that

$$\underline{5} \times \underline{29} = \underline{1} \quad (5 \times 29 = 145 = 4 \times 36 + 1)$$

but does $\underline{4}$ have an inverse? Instead of checking, observe that $\boxed{\underline{4} \times \underline{9} = \underline{0}}$

$\underline{4} \times$ something not $\underline{0}$ $= \underline{0}$

$\Rightarrow$ $\underline{4}$ cannot have an inverse. Indeed, otherwise we could write

$$\underbrace{\underline{4}^{-1} \times \underline{4}}_{=\underline{1}} \times \underline{9} = \underline{4}^{-1} \times \underline{0} = \underline{0}$$

so $\underline{9} = \underline{0}$, absurd.

In summary, we have seen 3 cases:

- The inverse exists (± 1 in $\mathbb{Z}$, $1+\sqrt{2}$ in $\mathbb{Z}[\sqrt{2}]$)
- The inverse "exists outside the ring", like $\frac{1}{2}$ for 2.
- The

the inverse cannot possibly exist, ex. $\underline{4}$ in $\mathbb{Z}_{36}$.

<u>Def.</u> Let R be a commutative ring, and $r \in R$. We say that r is "a zero divisor" if $r \neq 0$ and if there exists $r' \in R$, with $r' \neq 0$, such that $r \times r' = 0$.

<u>Ex.</u> $\underline{4}$ and $\underline{9}$ in $\mathbb{Z}_{36}$

<u>Rem.</u> If R is not commutative $\to$ "left zero divisor", "right zero divisor".. Could think of

$M = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $N = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ in a non-commutative setting,

here $M \cdot N = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, so both are zero divisors.

<u>Q.</u> Can you construct an example where r is a left zero divisor but not a right zero divisor

<u>Def.</u> A (commutative) ring R is said to be an integral domain if there are <u>no</u> zero divisors.

In other words, if R is an integral domain, we have the usual rule "$a \times b = 0 \Rightarrow a = 0$ or $b = 0$"

⚠ It is <u>false</u> in general for a ring!!!

<u>Examples</u>: $\mathbb{Z}$, $\mathbb{Z}[\sqrt{2}]$ are integral domains

- $\mathbb{Q}$, $\mathbb{R}$ also (see below)
- $\mathbb{Z} \times \mathbb{Z}$ <u>is not</u>. Why? $(0,1) \times (1,0) = (0,0)$
- $\mathbb{R}[X]$ (polynomials) <u>is</u>.
- $\mathbb{Z}_n$ is $\Leftrightarrow$ n is prime

II] Fields (definition)

<u>Def.</u> A field is a ring $(R, +, \times)$ such that
- R is commutative
- Every element $r \neq 0$ has an inverse for $\times$

<u>Rem. (terminology)</u>

* If R is not commutative, we say "division ring".

* An element that has a multiplicative inverse is called a "unit", confusing terminology $\neq$ unity (1).
The unity is a unit.... not all units are the unity!

<u>Examples</u>: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ for p prime.

An "abstract" way to construct fields is to consider quotient of rings by certain ideals.

<u>Thm</u> Let R be a commutative ring, I an ideal of R, and R/I the quotient ring (go back to the definition

If you have forgotten). Then

a) R/I is an integral domain $\Leftrightarrow$ I is a prime ideal

b) R/M is a field $\Leftrightarrow$ I is a maximal ideal

<u>Proof.</u> Reminder R/I is the set of all equivalence classes for the relation "being equal up to an element of I". There is a ring morphism

$$\begin{aligned} \pi : R &\longrightarrow R/I \\ r &\longmapsto \underline{r} \end{aligned}$$ the equivalence class

π is onto and what is its kernel?

$$\begin{aligned} \ker \pi &= \{ r \in R,\ \underline{r} = \underline{0} \} \\ &= \{ r \in R,\ r = 0 \text{ up to an element of } I \} \\ &= \{ r \in R,\ r - 0 \in I \} \\ &= \{ r \in I \} = I \end{aligned}$$

In particular, for any r, r' in R

$$\begin{aligned} \pi(r) \times \pi(r') = 0 &\Leftrightarrow \pi(r \times r') = 0 \\ &\Leftrightarrow r \times r' \in I \end{aligned}$$

Reminder: I is prime $\Leftrightarrow$ if $r \times r' \in I$, then $r \in I$ or $r' \in I$

a) 1) I prime $\Rightarrow$ R/I is an integral domain

- let a, b be in R/I, assume $a \times b = 0$, want to show $a = 0$ or $b = 0$.
- Since π is onto, can write $\begin{cases} a = \pi(r) \\ b = \pi(r') \end{cases}$ for some r, r' in R. Then $a \times b = 0$ means

$$\pi(r) \times \pi(r') = 0, \text{ so } r \times r' \in I \text{ (see above)}.$$

Since I is prime, we have $r \in I$ or $r' \in I$.
So $\pi(r) = \underline{0}$ or $\pi(r') = \underline{0}$.
hence $a = 0$ or $b = 0$, which is what we wanted

2) R/I is an integral domain $\Rightarrow$ I is prime

let r, r' be in R, such that $r \times r' \in I$. Want to show $r \in I$ or $r' \in I$.

Since $r \times r' \in I$, we have $\pi(r \times r') = \underline{0}$, so

$$\pi(r) \times \pi(r') = \underline{0}.$$

Since R/I is an integral domain, it means

$$\pi(r) = \underline{0} \quad \text{or } \pi(r') = \underline{0}$$

Since $\ker \pi = I$, it implies

$$r \in I \text{ or } r' \in I,$$

which is what we wanted.

<u>Exercise</u>: Try to prove b). Thm 16.35 in Textbook.