Remark. $\mathbb{H}$ is a division ring but not an integral domain, because it is not commutative.

Remark. Idempotent elements in integral domain: 0 and 1.

In $\mathbb{Z}_6$, we have 0, 1, . They pair up because $e^2 = e \Rightarrow (1-e)^2 = 1-e$.

If $S \leq R$ and S has identity e, then e is an idempotent in R.

Example. $R = M_3(\mathbb{R})$. $S = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{pmatrix} : a, b, c, d \in \mathbb{R}$. Then $S \leq R$. $S \neq \emptyset$ and S is closed under $+, -, \times$. S has the identity

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

So the identity of the subring doesn't have to be the identity of the parent ring, but it has to be idempotent.

Recall we are trying to construct a field F containing an integral domain D so that F is as small as possible.

Intuition. Consider $\frac{a}{b}, a, b \in \mathbb{Z}, b \neq 0$. We denote (a, b) as an element in $S = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : b \neq 0\}$. So we want to express that two fractions are the same by using $ad = bc$. We would use an equivalence relation to show that.

Lemma

Define $(a, b) \sim (c, d) \Leftrightarrow ad = bc$. Then $\sim$ is an equivalence relation on S.

Proof

(i) Reflective: $ab = ba$ is true by commutativity.

(ii) Symmetric: $ad = bc \Rightarrow^3 = da$ is true by commutativity.

(iii) Transitive: If $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, then $(a, b) \sim (e, f)$. Assume $ad = bc, cf = de$. Then

$$\begin{aligned} adcf &= bcde \\ acfd &= bced \\ acf &= bce \text{ by cancellation and } d \neq 0 \end{aligned}$$

Case. $c \neq 0$. Then $afc = bec \Rightarrow af = be$. Done.

Case. $c = 0$. Then $ad = bc = 0 \Rightarrow a = 0$ since $d \neq 0$. Also $cf = de \Rightarrow de = 0 \Rightarrow e = 0$ since $d \neq 0$. So $af = be = 0$.

$\square$

Notation. Define (the set of) the field F as $F = S/\sim$, which is the set of the $\sim$-equivalence classes of S.

Example. Suppose $D = \mathbb{Z}$, then denote the equivalence class of $(1, 2)$ as $[(1, 2)] = \{b = 2a : a, b \in \mathbb{Z}, b \neq 0\}$.

Example. In $\mathbb{Q}$, $\frac{1}{2} + \frac{1}{3} = \frac{5}{6}$. What if we use different names will it still be well-defined? Yes.

How can we add them?

$$[(a, b)] + [(c, d)] = [(ad + bc, ad)].$$

For multiplication,

$$[(a, b)] \times [(c, d)] = [(ac, db)].$$

We need to check they are well-defined.

Proof

Suppose $(a', b') \sim (a, b), (c', d') \sim (c, d)$. We need to show that $(a'd' + b'c', a'd') \sim (ad + bc, ad)$. Equivalence gives us $a'b = b'a, c'd = d'c$.

$$\begin{aligned}(a'd' + b'c')ad &= a'd'(ad + bc) \\ a'd'ad + b'c'ad &= a'd'ad + bca'd' \\ b'c'ad &= bc'a'd = bca'd'\end{aligned}$$

$\square$

Likewise for addition. So both are well-defined.

Addition is closed in S because $b, d \neq 0$ and D is a domain without zero divisors. Likewise for multiplication and subtraction.

We still need to show addition and multiplication are associative (omitted).

What is the additive identity? $[(a, b)] = [(0, 1)]$. b can be anything nonzero since $(0, 1) \sim (0, b)$. This works.

Additive inverse of $[(a, b)]$ is $[(-a, b)]$. We again can check it's true since $[(0, b^2)] \sim [(0, 1)]$.

What is the multiplicative identity? $[(a, b)] = [(1, 1)]$.

Multiplicative inverse of $[(a,b)]$ is $[(b,a)]$ since if $a=0$, then $[(a,b)] = [(0,b)] = [(0,1)]$ which is the zero so we can ignore. And $[(ab,ab)] = [(1,1)]$.

Commutative? Yes.

Division ring? If $[(a,b)] \neq 0_F$ then $a \neq 0$ and $[(b,a)]$ is the inverse.

So F is a field. We still need to show that F contains the D or has a subring that looks like D.