Basic concepts from ring theory

Def A ring homomorphism $\varphi: R \to S$ is a map of sets s.t. $\varphi(a+b) = \varphi(a) + \varphi(b)$

$$\varphi(ab) = \varphi(a)\varphi(b) \qquad \varphi(1) = 1$$

Def An (2-sided) ideal of a ring is a subset $I \subset R$ s.t.

$x+y \in I$ if $x,y \in I$ and $ax, xa \in I$ if $x \in I, a \in R$

we write $I \triangleleft R$.

(If we only assume $ax \in R$ we say I is a left ideal $I \triangleleft_\ell R$
$xa \in R$ . . . . right $I \triangleleft_r R$)

Def If $f: R \to S$ is a ring homomorphism, then

$\ker f = \{r \in R \mid f(r) = 0\} \triangleleft R$ and moreover

for $I \subset R$, $\quad I \triangleleft R \iff I = \ker f$ some $f: R \to S$ some S.

Recall: regarding $I \triangleleft R$ as a (normal) subgp of $(R,+)$

R/I has a ring structure via $(a+I)(b+I)$

$= ab + I$

and the canonical map $R \to R/I$ has kernel I.

<u>Examples</u> if $a \in R$, $\{x \in R \mid ax = 0\} \lhd_r R$

$\{x \in R \mid xa = 0\} \lhd_\ell R$

<u>Def</u> $I \lhd R$ is called maximal if $I \neq R$ and $I \subset J \lhd R \Rightarrow J = R$ or I.

<u>Proposition</u> Maximal ideals of any type exist in any (unital) ring.

<u>Pf</u>: Recall: Zorn's lemma:

if $(P, \leq)$ is a partially ordered set, a subset $C \subset P$ is called a <u>chain</u> if it is totally ordered

[$(C, \leq)$ totally ordered if $a, b \in C \Rightarrow a \leq b$ or $b \leq a$]

we say a chain $C \subset P$ has an upper bound if $\exists\ a \in P$ s.t. $a \geq b$ all $b \in C$

Zorn's Lemma: if $(P, \leq)$ is a PO set such that every chain has an upper bound then P has a maximal element

[$m \in P$ is a maximal element if $n \geq m \Rightarrow n = m$]

Consider $\mathcal{I}$ = set of proper ideals (left ideals / right...) partially ordered by inclusion.

Claim: chains in $\mathcal{I}$ have upper bounds.

Pf: if $C \subset \mathcal{I}$ is a chain then consider $$I = \bigcup_{J \in C} J$$

is an ideal since if $x, y \in I$ then $x \in J$, $y \in J'$, $J, J' \in C$ and WLOG $J \subset J' \Rightarrow x+y \in J' \subset I$

$I \neq R$ since $1 \notin I$ since $1 \notin J$ all $J \in C$.

$\square$

More ideal stuff:

If $I, J \triangleleft R$ (resp. $\triangleleft_\ell, \triangleleft_r$) then

$$I \cap J,\ I + J \triangleleft R$$

if $I, J \triangleleft R \Rightarrow IJ \triangleleft R$ $= \{\sum x_i y_i \mid x_i \in I, y_i \in J\}$

note $IJ \subset I \cap J$

$I^n \triangleleft R \qquad I^n \subset I$

$\mathbb{C} \times \{0\} \triangleleft \mathbb{C} \times \mathbb{C} \qquad p\mathbb{Z} \subset \mathbb{Z}$

if $I^2 = I$, is $I = R$?

how about if R is a domain?

$\mathbb{C}[\![x]\!] \subset \mathbb{C}[\![x^{1/n}]\!]$

$\mathbb{C}[\![y]\!]$

$R = \bigcup_n \mathbb{C}[\![x^{1/n}]\!] \qquad I = \bigcup_n x^{1/n} R$

if $S \subset R$ subset, (S) = smallest ideal containing S

R general $(S) = RSR = \left\{\sum r_i s_i r_i' \;\middle|\; s_i \in S,\ r_i, r_i' \in R\right\}$

R commutative $(S) = RS = SR$

If R any ring, consider the (unique) ring map

$$\mathbb{Z} \to R$$

the kernel has the form $(n) = n\mathbb{Z}$, $n \geq 0$

we define $\operatorname{char} R = n$

<u>Note:</u> if R is an integral domain, then n is prime.

<u>Fractions</u>

Let R be a commutative integral domain.

We define an equiv. relation on pairs $(a,b) \in R \times (R \setminus \{0\})$

by saying $(a,b) \sim (c,d)$ if and only if

$$ad = bc.$$

Let $F = R \times (R \setminus \{0\}) / \sim$

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc, bd)}$$

$$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac, bd)}$$

$$\overline{(a,b)}^{-1} = \overline{(b,a)}$$

$(\text{if } a \neq 0)$

Notation: $\frac{a}{b} = \overline{(a,b)}$ $\qquad \frac{ad}{bd} = \frac{a}{b}$

$a \mapsto \frac{a}{1}$

Note: we have a ring homomorphism $R \to F$ which is universal for maps to fields!

Universal property: if L is any field, together with a ring map $R \xrightarrow{\varphi} L$, then $\exists!\, F \to L$ s.t.

$$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr] & & L \\ & F \arrow[ur] & \end{tikzcd}$$

commutes.

$\frac{a}{b} \mapsto \varphi(a)\varphi(b)^{-1}$

if F' has same prop, can use above to get maps

$$\begin{tikzcd} R \arrow[r] \arrow[d] & F \\ F' \arrow[ur] & \end{tikzcd} \qquad \begin{tikzcd} R \arrow[r] \arrow[d] & F' \\ F \arrow[ur] & \end{tikzcd} \qquad \begin{tikzcd} R \arrow[r] \arrow[d] & F \\ F \arrow[ur, "?\, id"'] & \end{tikzcd}$$

$$\begin{tikzcd} R \arrow[r] \arrow[d] & F' \\ F' \arrow[ur, "?\, id"'] & \end{tikzcd}$$

Alternate Viewpoint

Start w/ R, we want to construct F

F is a field, we can describe maps $F \to L$ for any other field L (in bijection w/ maps $R \to L$)

$$\underline{\text{Fields}^{op}} \hookrightarrow \underline{\text{Fun}(\text{Fields}, \text{Sets})}$$

$$F \qquad\qquad \text{Hom}_{\text{field}}(F, -)$$

$$\text{Hom}_{\text{field}}(K, L) \xleftrightarrow{\text{bij}} \text{Hom}_{\text{Fun}}\left(\text{Hom}_{\text{Field}}(L, -), \text{Hom}_{\text{Field}}(K, -)\right)$$

$$\text{Hom}_{\text{field}}(K, L) = \text{Hom}_{\text{field}^{op}}(L, K)$$

Localization:

<u>Def</u> $S \subset R$ is a multiplicative set if $1 \in S$, and S is closed under multiplication

The ring $R[S^{-1}]$ is a ring together with a hom $R \to R[S^{-1}]$ s.t.

if T is any ring together with a map $R \xrightarrow{q} T$ s.t. $q(S) \subset T^*$ then $\exists!$ $R[S^{-1}] \to T$ s.t.

$$\begin{tikzcd} R \arrow[rr] \arrow[dr] & & T \\ & R[S^{-1}] \arrow[ur] & \end{tikzcd}$$

Construction is as before:

$$R \times S/\sim \qquad (r,s)\sim(r',s') \iff$$

$$t(rs'-sr')=0 \text{ some } t\in S.$$

$$\frac{r}{s}=(r,s) \qquad \frac{r}{s}+\frac{r'}{s'}=\frac{rs'+r's}{ss'}$$

$$\frac{r}{s}\,\frac{r'}{s'}=\frac{rr'}{ss'}$$

$$R \to R[S^{-1}] \qquad r \longmapsto \frac{r}{1}$$

__Claim:__ kernel of is $\{r\in R \mid sr=0 \text{ some } s\in S\}$