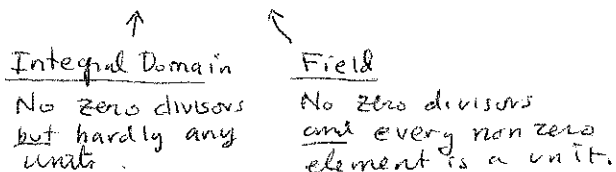


Section 7.5 Fields of Fractions.

Consider inclusion $\mathbb{Z} \subseteq \mathbb{Q}$



Goal Show that for any integral domain $R \exists$ field \mathbb{Q} with $R \subseteq \mathbb{Q}$.

Basic Plan :

① $\mathcal{D} = R - \{0\}$. (More generally, \mathcal{D} is a mult. closed set of elements that are not zero divisors)

② $\mathcal{F} = \{(r, d) \mid r \in R, d \in \mathcal{D}\}$

③ Define equiv. relation on \mathcal{F} : $(r, d) \sim (s, e)$ if $re = ds$.
Equiv. class containing (r, d) is denoted $\frac{r}{d}$.

④ Define Operations on \mathcal{Q} :

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \frac{a}{b} \frac{c}{d} = \frac{ac}{bd}$$

Check that this is well-defined.

⑤ Note \mathcal{Q} is a field with identity $\frac{1}{1}$.

$$\frac{a}{b} \frac{b}{a} = \frac{ab}{ab} = [(ab, ab)] = [(1, 1)] = \frac{1}{1}$$

⑥ Identify $R = \left\{ \frac{r}{1} \mid r \in R \right\}$. Then $R \subseteq \mathcal{Q}$ as desired.

Definition \mathcal{Q} is called The field of quotients of R .

\mathcal{Q} is the smallest field containing R in following sense:

Given injective ring homomorphism $\varphi: R \rightarrow F$ into a field, there is injective homomorphism

$$\begin{array}{ccc} & S & \\ & \downarrow \Phi & \\ R & \xrightarrow{\varphi} & F \end{array}$$

Such that $\Phi|_R = \varphi$.

Section 7.6 Chinese Remainder Theorem

Blanket assumption: All rings are commutative, have 1.

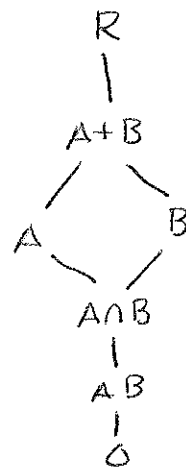
Suppose A, B are ideals in R :

New ideals:

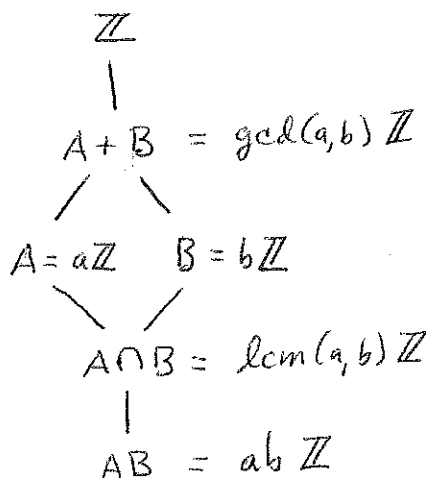
$$A+B = \{x+y \mid x \in A, y \in B\}$$

$$A \cap B$$

$$AB = (\{xy \mid x \in A, y \in B\})$$



Example:



$$A = (a)$$

$$B = (b)$$

$$AB = (ab)$$

Note $\gcd(a,b) = 1 \iff A+B = \mathbb{Z} \iff A \cap B = AB$

For general rings: $(A)+(B) = R \iff A \cap B = AB$
 $(a)+(b) = R \iff (a) \cap (b) = (ab)$

Definition $A, B \subseteq R$ are comaximal if $A+B = R$.

Theorem Suppose $a, b \in \mathbb{Z}^+$. The map $\mathbb{Z} \rightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ where $x \mapsto (x+a\mathbb{Z}, x+b\mathbb{Z})$ is a homomorphism with kernel $a\mathbb{Z} \cap b\mathbb{Z}$. If $\gcd(a,b) = 1$, it is surjective with kernel $a\mathbb{Z} \cap b\mathbb{Z} = ab\mathbb{Z}$. Thus there is an isomorphism

$$\mathbb{Z}/ab\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

$$x+ab\mathbb{Z} \mapsto (x+a\mathbb{Z}, x+b\mathbb{Z})$$

Proof (Surjective) Take $xa+yb=1$

$$lxa + kyb \mapsto (k+a\mathbb{Z}, l+b\mathbb{Z})$$

Consequence Given $a, b \in \mathbb{Z}$, rel. prime and $k, l \in \mathbb{Z}^+$
we can find a solution $x \in \mathbb{Z}$ to the system

$$\begin{cases} x \equiv k \pmod{a} \\ x \equiv l \pmod{b} \end{cases}$$

Historically such problems were considered by the ancient Chinese. Hence the above Theorem is called the Chinese Remainder Theorem. It generalizes as follows:

Theorem 17 (Chinese Remainder Theorem)

Suppose A_1, A_2, \dots, A_k are ideals in R . The map

$$R \longrightarrow R/A_1 \times R/A_2 \times \dots \times R/A_k$$

$$x \longmapsto (x+A_1, x+A_2, \dots, x+A_k)$$

is a ring homomorphism with kernel $A_1 \cap A_2 \cap \dots \cap A_k$.

If each pair A_i, A_j is comaximal, then map is surjective and $A_1 \cap A_2 \cap \dots \cap A_k = A_1 A_2 \dots A_k$, so

$$R/(A_1 A_2 \dots A_k) = R/A_1 \cap A_2 \cap \dots \cap A_k \cong R/A_1 \times R/A_2 \times \dots \times R/A_k$$

Corollary 18 Suppose $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ (prime factorization)

Then $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$

and $(\mathbb{Z}/n\mathbb{Z})^{\times} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^{\times} \times \dots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^{\times}$