date: monday, february 26, 2024

Review of Rings

Defⁿ: A ring R is a set with two binary operations (+ addition and × multiplication) such that for all $a, b \in R$.

says R is an abelian group under +:

① $a+b=b+a$
② $(a+b)+c=a+(b+c)$
③ There exists a $0 \in R$ such that $a+0=0+a=a$
④ For all $a \in R$, there exists $b \in R$ such that $a+b=0$ (usually write $-a$ for b)

⑤ $a(bc)=a(bc)$
⑥ $a(b+c)=ab+ac$
$(a+b)c=ac+bc$

Remark: A ring R is an abelian group with additional structure.

Special types of rings:

- a ring R has identity if exists an element $1_R \in R$ such that $a \cdot 1_R = 1_R \cdot a = a$
- R is a commutative ring if $ab=ba$ for all $a,b \in R$
- R is an integral domain if R has identity, is commutative, and if $ab=0$, then $a=0$ or $b=0$ (ie. no zero divisors)
- R is a division ring if R has an identity and if for all $a \in R$, $a \neq 0$, exists $a^{-1} \in R$ such that $a \cdot a^{-1}=1$ and $a^{-1}a=1$
- a ring R is a field if R has identity, R is commutative, and for all $a \in R$, $a \neq 0$, exists $a^{-1} \in R$ such that $a^{-1} \cdot a = 1$

Remark: We say $a \in R$, $a \neq 0$ is a unit if exists $a^{-1} \in R$ such that $a^{-1} \cdot a = 1$.

eg. $R=\mathbb{Q}[x]$ ← polynomials with coefficients in $\mathbb{Q}$ is an integral domain

eg. $\mathbb{Z}$ is an integral domain

eg. $\mathbb{R}, \mathbb{Z}_p$ p prime, $\mathbb{C}, \mathbb{Q}$ are fields

eg. $M_{n\times n}(\mathbb{R}) \leftarrow n\times n$ matrices is not an integral domain

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

eg. $E = \{2n \mid n \in \mathbb{Z}\} \leftarrow$ no identity

eg. $\mathbb{Z}_n$ (n not prime) is not an integral domain

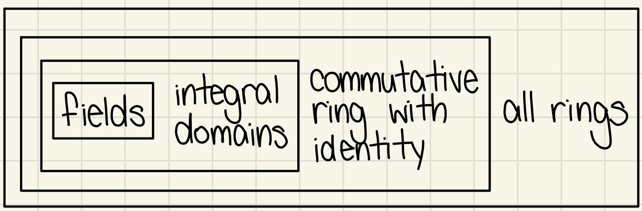
eg. $M_{n\times n}(\mathbb{R})$ is not a commutative ring

Fact: Every field is also an integral domain.

Proof

Suppose $ab=0$. If $a=0$, we are done. Suppose $a\neq 0$. So a^{-1} is in the field. So $a^{-1}(ab) = a^{-1}\cdot 0 = 0$. So $0 = a^{-1}(ab) = (a^{-1}a)b = 1_R \cdot b = b$.

$\square$



Subrings and Ideals

Def^n: A subring of a ring R is a subset S of R that is also a ring under the same operations.

(Subring Criteria) Let S be a subset of R. Then, S is a subring if

① $S \neq \emptyset$
② For all $a,b \in S$, $a-b \in S$
③ For all $a,b \in S$, $ab \in S$

An ideal is a special type of subring that has the "absorption property".

Def^n: A subset I of a ring R is an ideal if:

① $I \neq \emptyset$
② For $a,b \in I$, then $a-b \in I$
③ For $a \in I$, $r \in R$, then $\underbrace{ar \in I \text{ and } ra \in I}_{\text{if } R \text{ commutative, only need to check one}}$

eg. Let $R = \mathbb{Z}$ and $I = \{2024n \mid n \in \mathbb{Z}\}$. Claim: I is an ideal of $\mathbb{Z}$.
Check 3 conditions:
① $I \neq \emptyset$ since $2024 \cdot 1 \in I$
② Let $a,b \in I$. So $a = 2024m$ and $b = 2024n$ with $n,m \in \mathbb{Z}$.
So $a-b = 2024(m-n) \in I$.
③ Let $a \in I$. So $a = 2024m$. Let $r \in \mathbb{Z}$.
Then $ra = r(2024m) = 2024(rm) \in I$.

$\square$

Quotient Rings

We need ideals to form quotient rings.

Ideals play the same role as normal subgroups.

Set-Up: Let R be a ring with I an ideal. Note R is an abelian group under $+$. So I is a normal subgroup. So

$$R/I = \{a + I \mid a \in R\}$$

is defined as a group with addition: $(a+I)+(b+I) = (a+b)+I$.

Recall: $a+I = b+I \iff a-b \in I$. To give R/I a ring structure, need a multiplication.

Want: $(a+I)(b+I) = ab + I$.

Need to check that this is "well-defined" (our definition depends upon the choice of representative => we need to show this choice doesn't matter).

Lemma: Suppose $a_1+I=a_2+I$ and $b_1+I=b_2+I$. Then
$$a_1b_1+I=a_2b_2+I.$$

Proof

Given $a_1-a_2\in I$ and $b_1-b_2\in I$. Since I is an ideal,
$$(a_1-a_2)b_1=a_1b_1-a_2b_1\in I$$
and
$$a_2(b_1-b_2)=a_2b_1-a_2b_2\in I.$$
But then,
$$(a_1b_1-a_2b_1)+(a_2b_1-a_2b_2)=a_1b_1-a_2b_2\in I.$$
But this means
$$a_1b_1+I=a_2b_2+I.$$
$\square$

Theorem: If R is a ring with ideal I, then R/I is a ring under operations
$$(a+I)+(b+I)=(a+b)+I$$
$$(a+I)(b+I)=ab+I.$$

Trivial Ideals

Every ring R has at least two ideals $\{0\}$ and R is an ideal (trivial ideals).

Theorem: A field only has trivial ideals.

Proof

Suppose I is not the zero ideal. So exists $a\in I$ with $a\neq 0$. Since $a^{-1}\in R$, $a^{-1}a=1\in I$. But then for all $r\in R$, $r=r\cdot 1\in I$. So $R\subseteq I\subseteq R$.