April8

Thursday, April 8, 2021 12:27 PM

Def^n A ring is a set R with 2 binary operations

$$+ : R \times R \longrightarrow R \qquad \times : R \times R \longrightarrow R$$
$$(r,s) \longmapsto r+s \qquad (r,s) \longmapsto rs$$

s.t.

1) $(R,+)$ is an abelian group.
2) $\times$ is associative
3) Distributive law

$$a(b+c) = ab + ac \qquad (a+b)c = ac + bc$$

Rmk Additive identity 0

Multiplicative identity (if exists) is 1.

Def^n R a ring

- $a \in R$ is a zero divisor if $a \neq 0$ & $\exists\ b \neq 0$ w/ $ab = 0$
- If $R \ni 1 \neq 0$ then a is a unit if $\exists\ b \in R$ w/ $ab = 1$
- $R^\times \subseteq R$ is the set of units & a group under $\times$.

Observation

$\mathbb{Z}$, $\mathbb{R}[x]$, ...

Some nice examples are

$$* \left\{ \begin{array}{l} \bullet \ \text{Commutative} \\ \bullet \ \text{Have } 1 \neq 0 \\ \bullet \ \text{No zero divisors} \end{array} \right.$$

Def^{n}

A ring satisfying $(*)$ is called an integral domain.

Observation

- In $\mathbb{Z}$, have cancellation.

  If $2x = 2y \implies x = y$

  $nx = ny \implies x = y \quad (n \neq 0)$

- In $\mathbb{Z}/6\mathbb{Z}$ not true

  $\underset{6}{3 \cdot 2} \equiv \underset{12}{3 \cdot 4} \mod 6$

  But $2 \not\equiv 4 \mod 6$

  No cancellation

Integral domains have cancellation!

Prop 1) $a, b, c \in R$. $a \neq 0$. a not a zero divisor

Then if $ab = ac$

$\implies b = c$

2) R integral domain $a \neq 0$ in R

then. $ab=ac \implies b=c$

Proof

① ⇒ ② immediately.

Prove ①

$$ab=ac$$

Then $ab-ac=0$ (+ is abelian group)

Then $a(b-c)=0$ (distributive law)

$b-c=0$ (a not 0-divisor)

$b=c$ (+ abelian gp).

Easy & deep consequence.

Corollary

R be a finite integral domain.

Then R is a field.

Proof Let $\underline{\underline{a\neq 0}}$ Consider

$$\begin{aligned} R &\longrightarrow R \\ x &\longmapsto ax \end{aligned}$$

Function.

1) Injectivity

$$ax=ay \implies x=y.$$

2) Surjectivity follows b/c $|R|=|R|<\infty$

So $\exists$ x s.t. $ax=1$. So $a\in R^\times$.

So R a field.

Def^n Let R be a ring. An additive subgroup $S \subseteq R$ is called a Subring if it is closed under multiplication.

Examples

- $2\mathbb{Z} \subseteq \mathbb{Z}$. A subgroup.
  Multiplying 2 even #s gives an even number so a subring!
- $\mathbb{Z} \subseteq \mathbb{Q}$.
- $\mathbb{Q} \subseteq \mathbb{R}$.
- $\mathbb{R} \subseteq \mathbb{C}$
- $\underset{\substack{\uparrow \\ \text{Field}}}{\mathbb{C}} \subseteq \underset{\substack{\uparrow \\ \text{non commutative.}}}{\mathbb{H}}$

$a+bi \hookrightarrow a+bi+0j+0k.$

check details

$$\underset{\substack{\shortparallel \\ \text{Continuous functions} \\ \text{from } \mathbb{R}\to\mathbb{R}.}}{C(\mathbb{R})} \subseteq \text{Func}(\mathbb{R} \longrightarrow \mathbb{R})$$

Calc f, g continuous so are $f+g$ & fg.

Prop Let R be a ring w/ $1 \neq 0$
Then if R is a subring of a field F
then R is an integral domain.

Pf/ Commutative

$a, b \in R \subseteq F$. so $ab = ba$ ✓

No zero divisors

$0 \neq a \in R \subseteq F$.

If a is a zero divisor, it can't be a unit.

If $ab=0$ in R, $\Longrightarrow ab = 0$ in F

But $a \in F^{\times}$ so $b = 0$.

Subrings ↑ of integral domains are integral domains.
w/ $1 \neq 0$

Exercise

Remark This theorem has a converse:
If R is an integral domain, it is a subring of some field.

Example Let D be squarefree integer.

Define

$$\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}$$

$$a + b\sqrt{D} + \hat{a} + \hat{b}\sqrt{D}$$

$$= a + \hat{a} + (b + \hat{b})\sqrt{D}$$

$$(a+b\sqrt{D})(\hat{a}+\hat{b}\sqrt{D}) = a\hat{a} + a\hat{b}\sqrt{D} + \hat{a}b\sqrt{D} + b\hat{b}D$$

$$= (a\hat{a}+b\hat{b}D) + (a\hat{b}+\hat{a}b)\sqrt{D}.$$

$$(a+b\sqrt{D})^{-1} = \frac{a-b\sqrt{D}}{a^2-b^2D} \in \mathbb{Q}(\sqrt{D})$$

$\uparrow$ Nonzero bc if

$$a^2-b^2D=0 \Longrightarrow D=\frac{a^2}{b^2}=\left(\frac{a}{b}\right)^2$$

but D square free

$$(a+b\sqrt{D})\left(\frac{a-b\sqrt{D}}{a^2-b^2D}\right) = \frac{a^2-b^2D}{a^2-b^2D} = 1. \leftarrow$$

So $\mathbb{Q}(\sqrt{D})$ is a field!

Observe

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{D}) \quad \text{is a subring}$$

$$a \longmapsto a+0\sqrt{D}$$

(Suppose $D \equiv 2,3 \bmod 4$)

Define $\mathbb{Z}[\sqrt{D}] = \{a+b\sqrt{D} : a,b\in\mathbb{Z}\} \subseteq \mathbb{Q}(\sqrt{D})$

a subring called the ring of integers of $\mathbb{Q}(\sqrt{D})$.

Get

$$\begin{tikzcd}
\mathbb{Q} \arrow[r, hook] & \mathbb{Q}(\sqrt{D}) \arrow[l, dotted, bend right] \\
\mathbb{Z} \arrow[u, phantom, sloped, "\subseteq"] \arrow[r] & \mathbb{Z}[\sqrt{D}] \arrow[u, phantom, sloped, "\subseteq"]
\end{tikzcd}$$

What do factorizations, units, etc look like here?

↑ integral domain.

↑ ⚠ Depends on D

Tool for studying this question

$$\text{Norm} : \mathbb{Q}(\sqrt{D}) \longrightarrow \mathbb{Q}$$

$$(a+b\sqrt{D}) \longmapsto (a+b\sqrt{D})(a-b\sqrt{D})$$

$$= \underset{\uparrow}{a}^2 - \underset{\uparrow}{b}^2 \underset{\uparrow}{D} \in \mathbb{Q}$$

Facts

1) Norm is multiplicative.

$\text{Norm}(\alpha\beta) = \text{Norm}(\alpha)\,\text{Norm}(\beta)$ Exercise

⚠ Not additive!

2) $\alpha \in \mathbb{Z}[\sqrt{D}]$. Then $\text{Norm}(\alpha) \in \mathbb{Z}$.

Exercise

3) $\alpha \in \mathbb{Z}[\sqrt{D}]$.

α is a unit $\Longleftrightarrow$ $\text{Norm}(\alpha) = \pm 1$.

Proof of 3

$\Longrightarrow$). $\alpha^{-1} = \beta$ so $\alpha\beta = 1$

$N(\alpha\beta) = N(1+0\sqrt{D}) = 1$

multiplicative by ① $\longrightarrow$ $\parallel$

$N(\alpha)\cdot N(\beta)$.

$\uparrow \quad \uparrow$

Both in $\mathbb{Z}$.

So either both 1 or both -1.

$\Longleftarrow$ Know $\alpha = (a+b\sqrt{D}) \neq 0$ $\quad a, b \in \mathbb{Z}$

In $\mathbb{Q}(\sqrt{D})$

$$\alpha^{-1} = \frac{a-b\sqrt{D}}{\mathrm{Norm}(\alpha)} = \frac{a-b\sqrt{D}}{\pm 1} = \pm a \mp b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$$

So $\alpha \in \mathbb{Z}[\sqrt{D}]^{\times}$

Special Cases

1) $D = -1$

$\mathbb{Z}[\sqrt{D}] = \mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$

$\mathrm{Norm}(a+bi) = a^2 + b^2 = \pm 1$

$\uparrow \quad \uparrow$

$\Longleftrightarrow a = \pm 1 \quad b = 0 \quad \leftarrow \pm 1$

or $a = 0 \quad b = \pm 1 \quad \leftarrow \pm i$

$(\mathbb{Z}[i])^{\times} = \{\pm 1, \pm i\}$.

2) $D < -1$ $\qquad a + b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$ $\qquad -D \geq 2$

$$\text{Norm}(a+b\sqrt{D}) = \underset{\uparrow}{a^2} + \underbrace{b^2(-D)}_{\geq 2 \text{ if } b \neq 0} \quad \left(\begin{array}{c} = \pm 1 \\ \Updownarrow \\ a = \pm 1 \ \& \ b = 0 \end{array} \right)$$

So $\left(\mathbb{Z}[\sqrt{D}]\right)^\times = \{\pm 1\}$

3) $D = 2$ $\quad (D \geq 2)$

$$\text{Norm}(a+b\sqrt{D}) = \underset{\uparrow}{a^2} - \underset{\uparrow}{b^2} D$$ ← easier to make this $= \pm 1$

Ex $N(1+\sqrt{2}) = 1 - 2 = -1 \in \{\pm 1\}$

$(1+\sqrt{2}) \in \mathbb{Z}[\sqrt{2}]^\times$ $\quad \underbrace{(-1+\sqrt{2})(1+\sqrt{2})}_{\shortparallel}$

$\quad -1 - \sqrt{2} + \sqrt{2} + 2 = 1$

So $(1+\sqrt{2})^n \in \mathbb{Z}[\sqrt{2}]^\times$ $\forall n$

$\Longrightarrow \quad |\mathbb{Z}[\sqrt{2}]^\times| = \infty$

Polynomial Rings

Def$^{\underline{n}}$

R be a commutative w/ $1 \neq 0$. Then $R[x]$ is the set of polynomials w/ coefficients in R.

$$R[x] = \left\{ a_0 + a_1 x + \cdots + a_n x^n \;\middle|\; a_i \in R \right\}$$

Terminology

Let $f(x) = a_0 + a_1 x + \dots + a_n x^n$

$a_n \neq 0 \implies \deg f = n.$

$a_n = 1 \implies f$ is monic.

Operations

$$(a_0 + a_1 x + \dots + a_n x^n) + (b_0 + b_1 x + \dots + b_n x^n)$$

$$= (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_n + b_n)x^n$$

$$(\underline{a_0} + \underline{a_1 x} + \underline{a_2 x^2} + \dots + a_n x^n)(\underline{b_0} + \underline{b_1 x} + \underline{b_2} x^2 + \dots + b_n x^n)$$

$$a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \dots$$
$$+ (a_n b_n)x^{2n}$$

In general coefficient of x^i is

$$\sum_{j=0}^{i} a_j b_{i-j}$$

- Then $R[x]$ is a commutative ring whose identity is $1 = 1 + 0x + 0x^2 + \dots$

- R is a subring of $R[x]$ (as constant polynomials)

$$r = r + 0x + 0x^2 + \cdots$$

Ex

- $\mathbb{Z}[x] \subseteq \mathbb{Q}[x] \subseteq \mathbb{R}[x]$ subrings
- $(\mathbb{Z}/3\mathbb{Z})[x]$

$p(x) = x^2 + 2x + 1$

$q(x) = x^3 + x + 2$

$p(x) + q(x) = x^3 + x^2 + 3x + 3 = x^3 + x^2$

$p(x)q(x) = x^5 + 2x^4 + x^3 + x^3 + 2x^2 + x + 2x^2 + 4x + 2$

$= x^5 + 2x^4 + (1+1)x^3 + (2+2)x^2 + (1+4)x + 2$

$= x^5 + 2x^4 + 2x^3 + x^2 + 2x + 2$.

Coefficient Ring Makes a Difference

Example $x^2 + 1$

In $\mathbb{Z}[x]$: "Irreducible" Can't Factor!

In $\mathbb{C}[x]$: $(x^2 + 1) = (x+i)(x-i)$ Factors!

$= x^2 - (i^2)$

$= x^2 - (-1)$

In $(\mathbb{Z}/2\mathbb{Z})[x]$: $(x^2 + 1) = (x+1)^2$ Perfect Square!

"

x^2+2x+1

$2 \equiv 0 \mod 2$

$R[x]$ inherits properties from R.

Prop

R an integral domain, $f(x), g(x) \in R[x]$

1) $\deg(fg) = \deg f + \deg g$.

2) $(R[x])^\times = R^\times$ as constant polynomials.

3) $R[x]$ is an integral domain.

Proof

$f(x) = a_n x^n + \dots + a_0$ $\quad g(x) = b_m x^m + \dots + b_0$

& $a_n, b_m \neq 0$. $\left(\begin{array}{l}\deg f = n \\ \deg g = m\end{array}\right)$

$$fg = \underbrace{a_n b_m}_{\neq 0 \text{ b/c } R \text{ domain.}} x^{n+m} + \dots + a_0 b_0$$

so $\deg(fg) = m+n$ proves 1. & 3.

② $\deg 1 = 0$

If $fg = 1 \Rightarrow \deg(fg) = \deg f + \deg g = 0$

so $\deg f = \deg g = 0$

So $f, g \in R$. & $fg = 1$

so $f, g \in R^\times$.

$(R[x])^\times \subseteq R^\times$

Other direction is obvious.

Remarks

- If R has 0 divisors, so does $R[x]$
- $S \subseteq R$ a subring, then $S[x] \subseteq R[x]$ is too.

Group Rings

R a commutative ring w/ $1 \neq 0$.

$G = \{g_1, \dots, g_n\}$ a finite group w/ multiplicative group law.

Form

$$RG = R[G]$$

$$= \{a_1 g_1 + a_2 g_2 + \dots + a_n g_n \mid a \in R\}.$$

$$\sum a_i g_i + \sum b_i g_i = \sum (a_i + b_i) g_i$$

$$(ag_i)(bg_j) = (ab)g_k$$

$$g_k = g_i g_j$$

Use distributive law to apply to all elts.

Ex $\mathbb{Z}D_8$

$$\alpha = r + r^2 - 2s$$

$$\beta = -3r^2 + rs$$

$$\alpha + \beta = r - 2r^2 - 2s + rs$$

$$\alpha\beta = (r + r^2 - 2s)(-3r^2 + rs)$$

$$= r(-3r^2 + rs) + r^2(-3r^2 + rs) - 2s(-3r^2 + rs)$$

$$= \underline{\underline{-3r^3}} + \underline{r^2 s} - 3\underset{1}{\cancel{r^4}} + \underline{r^3 s} + 6\underset{\underset{\underline{r^2 s}}{\shortparallel}}{sr^2} - 2\underset{\underset{\underset{r^3}{\shortparallel}}{r^{-1}}}{\underline{srs}}$$

$$= -3 - 5r^3 + 7r^2 s + r^3 s.$$