Lecture 4: Rings, Basic Properties & Examples

Def'n ① A ring is a set R with two operations we call addition $+ : R \times R \to R$ and multiplication $\times : R \times R \to R$ which satisfies

(i.) $(R, +)$ is abelian group

(ii.) $\times$ is associative

(iii.) distributive laws hold

$$(a+b)\times c = a\times c + b\times c$$
$$a\times(b+c) = a\times b + a\times c$$

Remark: we often us juxtaposition to denote multiplication $A \times B = AB$

② R is commutative if $a \times b = b \times a$ for all $a, b \in R$

③ R is said to have an identity 1 if $1 \in R$ such that $1 \times a = a \times 1 = a$ for all $a \in R$.

Some texts assume $1 \in R$ for a ring as a default. Others would call a ring w/o identity a "Rng". If in doubt about a problem I've assigned then ask. We call a ring with unity (identity) a unital ring.

Def'n A unital ring with $1 \neq 0$ is called a division ring if every nonzero $a \in R$ has multiplicative inverse $a^{-1} \in R$ for which $a^{-1}a = aa^{-1} = 1$. A field is a commutative division ring.

Examples

commutative rings with 1

① $2\mathbb{Z}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_n = \mathbb{Z}/(n)$

$2\mathbb{Z}$: ring w/o identity.

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$: fields, but need $n = p$, a prime for $\mathbb{Z}_p$ a field ($\mathbb{Z}_6$ not a field)

Examples of Rings continued

② $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R},\ i^2 = j^2 = k^2 = -1$
$ij = k,\ jk = i,\ ki = j$
$ji = -k,\ kj = -i,\ ik = -j\}$

↑ Hamilton's Quaternions

$$(a+bi+cj+dk)^{-1} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}$$

Every nonzero quaternion is a unit, that is it has a multiplicative inverse. $\mathbb{H}$ is a skew-field.

③ If T is a ring and S is a set then $R = \mathcal{F}(S, T)$ the set of functions of form $f: S \to T$ forms a ring w.r.t. usual pointwise add. and mult.

$$(f + g)(x) = f(x) + g(x)$$
$$(fg)(x) = f(x)\,g(x)$$

If $1 \in T$ then $f(x) = 1$ for all $x \in S$ defines the multiplicative identity in $\mathcal{F}(S, T)$. Likewise $\mathcal{F}(S, T)$ will be commutative if T commutative.

④ Given ring R can form $R^{n\times n} = Mat_n(R)$ the set of $n \times n$ matrices with entries from R then define

$$(A+B)_{ij} = A_{ij} + B_{ij} \quad \text{and} \quad (AB)_{ij} = \sum_{k=1}^{n} A_{ik} B_{kj}$$

to see $R^{n\times n}$ forms a ring with unity if $1 \in R$.

⑤ Given ring R we form $R[x] = \{\sum_{n=0}^{\infty} c_n x^n \mid c_n \in R$, finitely many $c_n \neq 0\}$ this set of polynomials with coefficients in R in the indeterminant x forms a ring w.r.t. to usual addition and multiplication of polynomials.

Def'n/ Let R be a ring

(1.) We say $a \in R$ with $a \neq 0$ is a <u>zero divisor</u> if $\exists\, b \in R$ with $b \neq 0$ and $ab = 0$ or $ba = 0$.

(2.) If R is unital with $1 \neq 0$ then $u \in R$ is a <u>unit</u> if $\exists\, v \in R$ s.t. $uv = vu = 1$ in which case we write $v = u^{-1}$. The set of units is $R^\times$

Alternatively, we write $U(R)$ for $R^\times$ since U is for <u>units</u>.

<u>Examples of units and zero divisors</u>

① $\mathbb{Z}_n^\times = U(n) = \{ x \in \mathbb{Z}_n \mid \gcd(x, n) = 1 \}$

② If $\mathbb{F}$ is field then $\mathbb{F}^\times = \mathbb{F} - \{0\}$

③ Given ring R then $\mathcal{F}(S, R)$ where S is a nonempty set has many divisors of zero since $S_1, S_2 \subseteq S$ with $S_1 \cap S_2 = \emptyset$ give <u>characteristic</u> functions. Note

$$\chi_U(x) = \begin{cases} 1 & \text{if } x \in U \\ 0 & \text{if } x \notin U \end{cases}$$

defines $\chi_U : S \longrightarrow R$ where $1 \neq 0$ is unity in R

Then $(\chi_{S_1}\, \chi_{S_2})(x) = \chi_{S_1}(x)\chi_{S_2}(x) = 0$ for all $x \in S$

yet $\chi_{S_1}, \chi_{S_2} \neq 0$ since $\chi_{S_j}(x) = 1 \neq 0$ for each $x \in S_j$ for $j = 1, 2$.

④ $\mathbb{Z}^\times = \{-1, 1\}$ and $\mathbb{Z}$ has no zero divisors.

⑤ If R is commutative ring with $1 \neq 0$ then $A \in R^{n \times n}$ is a unit iff $\det(A) \in R^\times$.

Def^{n}/ A commutative ring with $1 \neq 0$ is called an integral domain if it has no zero divisors

Proposition:

Let R be commutative ring with $1 \neq 0$.

(1.) if a is not a zero divisor and $ab = ac$ then either $a = 0$ or $b = c$.

(2.) if $ab = ac$ for $a \neq 0$ in an integral domain then $b = c$. (cancellation property)

(3.) a zero divisor is not a unit and a unit is not a zero divisor.

Proof: (1.) Suppose $ab = ac$ for some $a, b, c \in R$ where a is not a zero divisor and $a \neq 0$ then $ab - ac = 0$ hence $a(b-c) = 0$ thus $b - c = 0$ as a is not zero divisor and thus $b = c$.

(2.) If $ab = ac$ for $a \neq 0$ then since the integral dom. $\clubsuit$ has no zero divisors we find $b = c$ by (1.)

(3.) Suppose $ab = 0$ where $a, b \neq 0$. If a^{-1} such that $a^{-1}a = 1$ then $a^{-1}ab = 1b = b$ thus $a^{-1}(ab) = a^{-1}(0) \Rightarrow b = 0$ $\rightarrow\!\leftarrow$.

Conversely, suppose $a \neq 0$ and a^{-1} exists then if $b \neq 0$ has $ab = 0$ we obtain $a^{-1}ab = a^{-1}(0) \Rightarrow b = 0$ $\rightarrow\!\leftarrow$.

Th^m/ Any finite integral domain is a field

Proof: an integral domain is a commutative ring with $1 \neq 0$. It remains to show every nonzero element in

$$R = \{0, x_2, x_3, \ldots, x_n\}$$

is a unit. Let $a \neq 0$ and define $f : R \longrightarrow R$ by $f(x) = ax$ then $f(x) = f(y) \Rightarrow ax = ay \Rightarrow x = y$ thus f is injective function on the finite set R hence f is surjective and so $\exists x \in R$ such that $f(x) = 1 \Rightarrow ax = 1 \Rightarrow a^{-1} = x$. Thus R is field. //

Remark: my LECTURE 21 from Math 421 of 2018 gives a slightly different proof for Th^m 4.1.33 (p. 127)

Def^n/ A subring of the ring R is a subgroup of $(R, +)$ that is closed under multiplication. (However, if we require $1 \in R$ then the subring must also contain 1.)

Th^m/ (Subring Test)

A subset S of a ring R is a subring of R if for $a, b \in S$ we have $a - b, ab \in S$.

Remark: Th^m 4.1.14 of my LECTURE 21, Math 421 notes 2018 also require $1 \in S$ since those notes are based on the definition of ring which assumes $1 \in R$. I should show Examples 4.1.15, 4.1.16, 4.1.17 to see the difference in terminology. In summary, our "RING" IS MY NOTES "RNG"

Examples of Subrings

(1.) $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subset \mathbb{R}$$

(2.) $n\mathbb{Z}$ for $n \in \mathbb{N} - \{1\}$ is subring of $\mathbb{Z}$
(but, not a subring with unity)

Note $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ not a subring of $\mathbb{Z}$.

(3.) $\underbrace{C^\infty(\mathbb{R})}_{\text{smooth functions on } \mathbb{R}} \subset \underbrace{C^2(\mathbb{R})}_{\text{twice cont. differentiable functions on } \mathbb{R}} \subset \underbrace{C^1(\mathbb{R})}_{\text{continuously diff. functions on } \mathbb{R}} \subset \underbrace{C^0(\mathbb{R})}_{\text{continuous functions on } \mathbb{R}} \subset \underbrace{\mathcal{F}(\mathbb{R})}_{\text{functions on } \mathbb{R}}$

each function space above forms a subring of the set of all functions on $\mathbb{R}$; $\mathcal{F}(\mathbb{R}) = \mathcal{F}(\mathbb{R}, \mathbb{R})$.

(4.) If S is subring of R then $S[x]$ is subring of $R[x]$

(5.) If S is subring of R then $M_n(S) \subset M_n(R)$ is naturally a subring w.r.t. matrix add & mult.

(6.) If $UT_n(R)$ is the set of upper triangular matrices with entries from the ring R then we can show $UT_n(R)$ is subring of $R^{n \times n} = M_n(R)$.

CLAIM: if $S \subset R$ where R is ring and S is a subring then $S[x]$ is subring of $R[x]$

Proof: let $a(x), b(x) \in S[x]$ then $\exists\, a_n, b_n \in S$ for which $\sum_{n=0}^{\infty} a_n x^n = a(x)$ and $\sum_{n=0}^{\infty} b_n x^n = b(x)$ where only finitely many $a_n, b_n \neq 0$. Then,

$$a(x) - b(x) = \sum_{n=0}^{\infty} (a_n - b_n) x^n \in S[x]$$

since $a_n, b_n \in S \Rightarrow a_n - b_n \in S$ as S is subring.

Moreover,

$$a(x)\, b(x) = \sum_{n=0}^{\infty} \sum_{k=0}^{n} a_k\, b_{n-k}\, x^n$$

$$= \sum_{n=0}^{\infty} (a_0 b_n + a_1 b_{n-1} + \cdots + a_{n-1} b_1 + a_n b_0) x^n$$

Thus $a(x)\, b(x) \in S[x]$ since $a_k, a_{n-k} \in S \Rightarrow a_k a_{n-k} \in S$ as S is closed under multiplication.

Remark: §7.2 of Dummit & Foot has nice run-down of all the standard terminology for the polynomial ring.

$$a(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

with $a_n \neq 0$ has $\deg(a(x)) = n$, a_n is the leading term

with $a_n = 1$ is called monic

PROPOSITION

Let R be an integral domain with non zero $P(x), q(x)$ in $R[x]$. Then,

(1.) $\deg(P(x)q(x)) = \deg(P(x)) + \deg(q(x))$

(2.) the units of $R[x]$ are $R^\times$ viewed as constant polynomials within $R[x]$

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

PROOF (1) Suppose $P(x) = a_m x^m + \cdots + a_0$ and $q(x) = b_n x^n + \cdots + b_0$ are non zero polynomials in $R[x]$ where R is int. dom. then $P(x)q(x) = a_m b_n x^{m+n} + \cdots + a_0 b_0$ hence $a_m b_n$ is the leading term in $P(x)q(x)$ as $a_m, b_n \neq 0$ implies $a_m b_n \neq 0$ since R has no zero divisors.

Thus $\deg(P(x)q(x)) = m+n = \deg(P(x)) + \deg(q(x))$.

(2.) If $P(x)q(x) = a_m b_n x^{m+n} + \cdots + a_0 b_0 = 1$ * then all coefficients $a_m, b_n = 0$ for $m, n \geq 1$ by equating coefficients of *. Thus $a_0 b_0 = 1$ and so $a_0, b_0 \in R^\times$ and $P(x) = a_0$, $q(x) = b_0$ and (2) follows.

(3.) If $P(x)q(x) = 0$ where $P(x), q(x) \neq 0$ then $a_m b_n x^{m+n} + \cdots + a_0 b_0 = 0 \Rightarrow a_m b_n = 0$ where $a_m, b_n \neq 0$ (I'm still assuming a_m and b_n are leading terms of $P(x), q(x)$) thus R has zero divisors $a_m, b_n \longrightarrow\!\!\leftarrow$ since R int. dom has no zero div.

Group Rings (§7.2 of Dummit & Foote)

Given a finite group $G = \{g_1, g_2, \ldots, g_n\}$ and a commutative ring R with $1 \neq 0$ then the group ring RG is given by

$$RG = \{a_1 g_1 + a_2 g_2 + \cdots + a_n g_n \mid a_i \in R,\ 1 \leq i \leq n\}$$

$$= \{a_1 + a_2 g_2 + \cdots + a_n g_n \mid a_i \in R \text{ if } g_i = e_G\}$$

Addition and multiplication are defined by:

① $(a_1 g_1 + \cdots + a_n g_n) + (b_1 g_1 + \cdots + b_n g_n) = (a_1 + b_1) g_1 + \cdots + (a_n + b_n) g_n$

$$\left(\sum_{i=1}^{n} a_i g_i\right) + \left(\sum_{i=1}^{n} b_i g_i\right) = \sum_{i=1}^{n} (a_i + b_i) g_i$$

② $(a_1 g_1 + a_2 g_2 + \cdots + a_n g_n)(b_1 g_1 + b_2 g_2 + \cdots + b_n g_n) =$

$$= a_1 b_1 g_1 g_1 + a_1 b_2 g_1 g_2 + \cdots + a_1 b_n g_1 g_n +$$

$$+ a_2 b_1 g_2 g_1 + a_2 b_2 g_2 g_2 + \cdots + a_2 b_n g_2 g_n + \cdots$$

$$+ a_n b_1 g_n g_1 + a_n b_2 g_n g_2 + \cdots + a_n b_n g_n g_n$$

Or, if you like to write way less, we define multiplication by $(a g_i)(b g_j) = ab\, g_k$ where $g_i g_j = g_k$ then extend to all formal sums via the distributive laws.

Th^{m}/ RG forms a ring w.r.t. the above addition and multiplication

Remark: RG is commutative iff G is an abelian group.

In the case $R = \mathbb{R}$ the group ring

$$\mathbb{R}G = g_1\mathbb{R} \oplus g_2\mathbb{R} \oplus \cdots \oplus g_n\mathbb{R}$$

external direct sum $\cong \mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R} = \mathbb{R}^n$

$g_j \longleftrightarrow e_j$ gives the isomorphism

$\{g_1, g_2, \ldots, g_n\} \subseteq \mathbb{R}G$ is LI

Th^m/ If $|G| > 1$ then RG has zero divisors.

Proof: let $g \in G$ have order $m > 1$. Then

$$(1-g)(1+g+\cdots+g^{m-1}) = 1-g^m = 1-1 = 0$$

hence $1-g$ is a zero divisor. //

Examples of Group Rings

(1.) $\mathbb{Z}G$ is the integral group ring of G

(2.) $\mathbb{Q}G$ is the rational group ring of G

(3.) $G = \{1, j\}$ where $j^2 = 1$ is cyclic group of order 2

then $\mathbb{R}G = 1\cdot\mathbb{R} \oplus j\mathbb{R} = \{a + bj \mid a, b \in \mathbb{R}\}$

form the hyperbolic #'s. Note $\underbrace{(1+j)(1-j) = 0}$ zero divisors.

as the Th^m above revealed

(4.) $Q_8 = \{1, -1, i, -i, j, -j, h, -h\}$ the quaternion 8-group gives $\mathbb{R}Q_8 \neq \mathbb{H}$ ← quaternions

since $\mathbb{H}$ has no divisors of zero.