MA 450: Honors Abstract Algebra Notes

Lecturer: Linquan Ma
Transcribed by Josh Park

Fall 2024

Contents

Lecture 32 (11/8)

12 Introduction to Rings

12.1 Motivation & Definition

Definition 12.1 (Ring)**.** A ring R is a set with two binary operations: $a+b$ and $a \cdot b = ab$ such that for all $a, b, c \in R$,

1. $a + b = b + a$
2. $(a+b)+c = a+(b+c)$
3. $\exists$ an additive identity 0, $a + 0 = a$
4. $\exists$ an element $-a \in R$ such that $a + (-a) = 0$
5. $(ab)c = a(bc)$
6. $a(b+c) = ab + ac$

   $(b+c)a = ba + ca$

So a ring is an abelian group under addition, and also has an associative multiplication that is left and right distributive over addition.

- The multiplication need not be commutative. When it is, we say the ring is commutative.
- A unity (or identity): a nonzero element that is an identity under multiplication.
- unit: a nonzero element of a commutative ring with identity that has a multiplicative inverse.
- In R, $a \mid b$ if $\exists c \in R$ such that $b = ac$.
- $n \in \mathbb{Z}_{>0}$, $na = \underbrace{a + a + \cdots + a}_{\text{n times}}$

12.2 Examples of Rings

Example 12.1. $(\mathbb{Z}, +\times)$ is a commutative ring with identity and units $= \pm 1$

Example 12.2. $(\mathbb{Z}_n, +\times)$ is a commutative ring with identity and units $= U(n)$

Example 12.3. $(\mathbb{Z}[x], +\times)$ is a commutative ring with identity

Example 12.4. $(\mathbb{M}_2[\mathbb{Z}], +\times)$ is a non-commutative ring with identity

Example 12.5. $(2\mathbb{Z} = \{\text{even integers}\}, +\times)$ is a comm ring without identity

Example 12.6. $(\{\text{continuous functions on } \mathbb{R}, +\times\})$ is a comm ring with identity $f(x) = 1$

Example 12.7. ($\{$continuous functions on $\mathbb{R}$ whose graphs pass through $(1, 0), +\times\}$) is a comm ring without identity

Note $f(1) = 0$, $g(1) = 0$, $f + g, fg$

Example 12.8 (Direct sum). Let $R_1, R_2, \ldots, R_n$ be rings. Construct

$$R_1 \oplus R_2 \oplus \cdots \oplus R_n = \{(r_1, r_2, \ldots, r_n) \mid r_i \in R_i\}$$

with component-wise addition and multiplication. This ring is called the direct sum of $R_1, R_2, \ldots, R_n$.

12.3 Properties of Rings

Theorem 12.1 (Rules of Multiplication). For all $a, b, c \in R$,

1. $a \cdot 0 = 0 \cdot a = 0$
2. $a(-b) = (-a)b = -(ab)$
3. $(-a)(-b) = ab$
4. $a(b - c) = ab - ac$

   $(b - c)a = ba - ca$
5. $(-1)a = -a$
6. $(-1)(-1) = 1$

Note. Properties 5 and 6 only hold if R has an identity 1

Proof of property 1. Clearly $0 + a0 = a0 = a(0 + 0) = a0 + a0$, so by cancellation $0 = a0$ and similarly $0a = 0$ □

Theorem 12.2 (Uniqueness of the Unity and Inverses). If a ring R has a unity, it is unique. If a ring element has a multiplicative inverse, it is unique.

Proof. 1, 1' $\implies$ 1=1·1' = 1'

$a \quad ab = ba = 1$

$\quad ac = ca = 1$

$c = c \cdot 1 = c(ab) = (ca)b = 1 \cdot b = b$ □

Warning. In general, $ab = ac \not\Longrightarrow b = c$ (cancellation rule does not hold in general for multiplication).

Example 12.9. In $\mathbb{Z}_6$, notice $2 \cdot 3 = 0 = 3 \cdot 0$ but $2 \neq 0$

12.4 Subrings

Definition 12.2 (Subring). A subset $S \subseteq R$ is a subring of R if S is itself a ring with the operations of R

Theorem 12.3 (Subring Test). A nonempty subset S of a ring R is a subring if S is closed under subtraction and multiplication.

i.e. if $a, b \in S$ then $a - b \in S$ and $ab \in S$

Example 12.10 (Trivial Subrings). $\{0\}$ and R will always be subrings of any ring R.

Example 12.11. $\{0, 2, 4\} \subseteq \mathbb{Z}_6$ is a subring

1 is the identity in $\mathbb{Z}_6$

4 is the identity in $\{0, 2, 4\}$ $(0 \cdot 4 = 0,\ 2 \cdot 4 = 2,\ 4 \cdot 4 = 4)$

Example 12.12. $n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$ is a subring of $\mathbb{Z}$ that does not have any identity (if $n \neq 1$).

Lecture 33 (11/13)

Example 12.13. The set of Gauss integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$.

13 Integral Domains

13.1 Definition and Examples

Definition 13.1 (Zero-Divisors). A zero-divisor is a nonzero element x of a commutative ring R such that there is a nonzero element $y \in R$ with $xy = 0$.

Example 13.1. In $R = \mathbb{Z}_6$, $x = 2$ is a zero-divisor

Definition 13.2 (Integral Domain). An integral domain is a commutative ring with unity and no zero-divisors.

Thus, in an integral domain, $ab = 0 \implies a = 0$ or $b = 0$.

Example 13.2. The ring of integers $\mathbb{Z}$ is an integral domain.

Example 13.3. The ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is an integral domain.

Example 13.4. The ring $\mathbb{Z}[x]$ of polynomials with integer coefficients is an integral domain.

Example 13.5. The ring $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ is an integral domain.

Example 13.6. The ring $\mathbb{Z}_p$ where p is prime is not an integral domain.

Non-Example 13.1. The ring $\mathbb{Z}_n$ where n is not prime is not an integral domain.

Note. Write $n = ab$ where $1 < a, b < n \implies a, b$ are both zero-divisors in $\mathbb{Z}_n$.

Non-Example 13.2. The ring $\mathbb{Z} \oplus \mathbb{Z}$ is not an integral domain.

Note. $(1, 0) \times (0, 1) = (0, 0)$

Theorem 13.1 (Cancellation). Let R be an integral domain. If $a \neq 0$, then $ab = ac \implies b = c$

Proof. $ab = 0, \quad a \neq 0 \implies 0 = a^{-1}ab = b$ □

13.2 Fields

Definition 13.3 (Field). A <u>field</u> is a commutative ring with unity in which every nonzero element is a unit

Fact. Every field is an integral domain.

Examples. $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}_p$

Note ($\mathbb{Z}_p$). $1 \leq a < p$ then $gcd(a, p) = 1$; $as + pt = 1 \implies as = 1 \bmod p \implies a$ is a unit in $\mathbb{Z}_p$

Non-Examples. $\mathbb{Z}$, $\mathbb{Z}[i]$

Theorem 13.2. A finite integral domain is a field.

Proof. $a \in R$ if $a = 1 \implies a^{-1} = 1$

Suppose $a \neq 1$. Consider $a, a^2, a^3, \ldots$

R is finite $\implies \exists i > j$ such that $a^i = a^j$

$a^i = a^j \cdot a^{i-j} \implies a^{i-j} = 1 \implies a \cdot (a^{i-j-1}) = 1 \implies a^{-1} = a^{i-j-1}$ exists in R. □

Example 13.7. $\mathbb{Z}_3[i] = \{a + bi \mid a, b \in \mathbb{Z}_3\}$ is a field with 9 elements.

$(a + bi)^{-1} = \frac{a-bi}{a^2+b^2}$ need to check if $a, b \in \mathbb{Z}_3$ then $a^2 + b^2 \neq 0$ in $\mathbb{Z}_3$ (unless $a = b = 0$).

$(1 + 2i)^{-1}$ in $\mathbb{Z}_3[i]$ is $\frac{1-2i}{1+4} = (1 - 2i) \cdot 2^{-1} = 2(1 + 1 \cdot i) = 2 + 2i$

Example 13.8. $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a field.

$$\begin{aligned}(a+b\sqrt{2})^{-1} &= \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2-2b^2} \\ &= \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2} \quad (a^2-2b^2 \neq 0)\end{aligned}$$

Definition 13.4 (Characteristic)**.** The characteristic of a ring R is the least positive integer $\text{char}(R) = n$ such that $\underbrace{nx}_{\sum^n x} = 0$ for all $x \in R$. If no such integer exists, we say R has characteristic 0.

Examples. $\text{char}(\mathbb{Z}) = 0,\ \text{char}(\mathbb{Z}_n) = n,\ \text{char}(\mathbb{Z}_2) = 2$

Theorem 13.3. Let R be a ring with unity 1. If 1 has infinite order under addition, then $\text{char}(R) = 0$. If 1 has order n under addition, then $\text{char}(R) = n$

Proof. $n \cdot 1 = 0 \implies n \cdot x = \sum^n x = x \cdot \sum^n 1 = x \cdot 0 = 0$ □

Theorem 13.4. If R is an integral domain, then $\text{char}(R)$ is either 0 or prime.

Proof. Suppose $\text{char}(R) = n \geq 0 \iff$ 1 has finite order n under addition by Thm. If $n = st$ where $1 < s, t < n$, then

$$0 = n \cdot 1 = (s \cdot 1)(t \cdot 1)$$

so $s \cdot 1 = 0$ or $t \cdot 1 = 0$. Since $\text{char}(1) = n$, it must be that $s = n$ or $t = n$. However, $s, t < n$. □

14 Ideals and Factor Rings

14.1 Ideals

Definition 14.1 (Ideal)**.** A subring I of a ring R is called a (two-sided) ideal of R if $\forall r \in R, \forall a \in I$ we have $ra \in I$ and $ar \in I$

- So a subring of R is an ideal if it "absorbs" elements of R
- An ideal of R is called a proper ideal if $I \neq R$

Theorem 14.1 (Ideal Test)**.** A nonempty subset I of a ring R is an ideal if

1. $a - b \in I$ whenever $a, b \in I$
2. $ra, ar \in I\ \forall a \in I, r \in R$

Example 14.1. For any ring R, $\{0\}$ and R are ideals.

Example 14.2. $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$ for all $n \in \mathbb{Z}$

Example 14.3. $\langle a \rangle := \{ra \mid r \in R\}$ is an ideal of R for all commutative rings with unity and $a \in R$. This is called the principal ideal generated by a.

Example 14.4. $R = \mathbb{R}[x] \quad I = \langle x \rangle = \{\text{polynomials with constant term } 0\}$

Example 14.5. Let R be a commutative ring with unity, $a_1, a_2, \ldots, a_n \in R$. Then

$$I = \left\{ \sum^{n} r_i a_i \mid r_i \in R \right\}$$

is an ideal of R, called the ideal generated by $a_1, a_2, \ldots, a_n \in R$.

Lecture 34 (11/15)

Example 14.6. $R = \mathbb{Z}[x]$, $I = \langle x, 2 \rangle = \{\text{polynomials with even constant terms}\}$

Non-Example 14.1. Let $R = \{\text{real valued functions in one variable}\}$. Then,

$$S = \{\text{differentiable functions in R}\}$$

is a subring of R but S is NOT an ideal of R.

14.2 Factor Rings

Theorem 14.2 (Existence of Factor Rings)**.** Let R be a ring and let A be a subring of R. Then the set of cosets $\{r + A \mid r \in R\}$ is a ring under the operation

- $(s + A) + (t + A) = s + t + A$ and
- $(s + A)(t + A) = st + A$

if and only if A is an ideal of R.

Pf sketch. A is an ideal of $R \implies$ addition and multiplication of cosets are well-defined (i.e. do not depend on the choice of representative)

Conversely, if A is not an ideal, then $\exists a \in R, r \in R$ such that $ar \notin A \neq A$.

Then

$$(a + A)(r + A) = ar + A \neq A$$

but

$$(a + A)(r + A) = (0 + A)(r + A) = 0 \cdot r + A = 0 + a = A \quad (\Rightarrow\!\Leftarrow)$$

□

Example 14.7. $n\mathbb{Z}$ ideal of $\mathbb{Z}$.

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \cdots, (n-1) + n\mathbb{Z}\} \cong \mathbb{Z}$$

$$\begin{aligned}(k + n\mathbb{Z}) + (\ell + n\mathbb{Z}) &= k + \ell + n\mathbb{Z} \\ &= (k+\ell) \bmod n + n\mathbb{Z}\end{aligned}$$

$$(k + n\mathbb{Z}) \cdot (\ell + n\mathbb{Z}) = k\ell + n\mathbb{Z}$$

Example 14.8. $2\mathbb{Z}/6\mathbb{Z} = \{0 + 6\mathbb{Z},\ 2 + 6\mathbb{Z},\ 4 + 6\mathbb{Z}\}$

Note. In general,

$$m \,\big|\, n \implies m\mathbb{Z}/n\mathbb{Z} = \left\{0 + n\mathbb{Z}, m + n\mathbb{Z}, 2m + n\mathbb{Z}, \cdots, m\left(\frac{n}{m} - 1\right) + n\mathbb{Z}\right\}$$

Example 14.9. $R = \left\{ \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \,\middle|\, a_i \in n\mathbb{Z} \right\}, \quad I = \{\text{matrices in } R \text{ with even entries}\}$

Exercise. Let $R/I = \left\{ \begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} + I \,\middle|\, r_i \in \{0, 1\} \right\}$. Prove $R/I \cong M_2\{\mathbb{Z}_2\}$.

Example 14.10 (★). $\mathbb{Z}[i]$ and $\langle 2 - i\rangle$

$\mathbb{Z}[i]/\langle 2-i\rangle = \{0 + \langle 2-i\rangle,\quad 1 + \langle 2-i\rangle,\quad 2 + \langle 2-i\rangle,\quad 3 + \langle 2-i\rangle,\quad 4 + \langle 2-i\rangle\}$

$$\begin{aligned} 5 = (2-i)(2+i) &\implies 5 \in \langle 2-i\rangle \\ &\implies 5 + \langle 2-i\rangle = 0 + \langle 2-i\rangle \\ i = 2 - (2-i) &\implies i + \langle 2-i\rangle = 2 + \langle 2-i\rangle \\ &\implies 2i + \langle 2-i\rangle = 4 + \langle 2-i\rangle \\ &\cdots \text{ etc } \cdots \end{aligned}$$

$\mathbb{Z}[i]/\langle 2-i\rangle \overset{\cong}{\to} \mathbb{Z}_5$

$a + \langle 2-i\rangle \mapsto a \bmod 5$

$i + \langle 2-i\rangle \mapsto 2 \bmod 5$

$a + bi \underset{\bmod (2-i)}{=} (a \bmod 5) + 2b = (a + 2b) \bmod 5$

Example 14.11. $\mathbb{R}[x]$ and $\langle x^2+1\rangle$

$$\begin{aligned}\mathbb{R}[x] &= \{g(x)+\langle x^2+1\rangle \mid g(x)\in\mathbb{R}[x]\}\\ &= \{ax+b+\langle x^2+1\rangle \mid a,b\in\mathbb{R}\}\cong\mathbb{C}\end{aligned}$$

$$\begin{aligned}\implies \mathbb{R}\,/\,\langle x^2+1\rangle &\cong \mathbb{C}\\ \mathbb{R}&\to\mathbb{R}\\ x+\langle x^2+1\rangle &\mapsto i\end{aligned}$$

$(x+\langle x^2+1\rangle)^2 = x^2+\langle x^2+1\rangle = -1+\langle x^2+1\rangle$

Lecture 35

Definition 14.2 (Prime Ideal, Maximal Ideal). A prime ideal P of a commutative ring R is a proper ideal of R such that if $a,b\in R$ and $ab\in P$,

Lecture 36

Theorem 14.3. Let R be a commutative ring with 1. Let A be an ideal of R. Then,

1. $R\,/\,A$ = integral domain $\iff$ $A=$ prime
2. $R\,/\,A$ = field $\iff$ $A=$ maximal

Proof. 1. $R\,/\,A$ = integral domain

$\iff$ $(a+A)(b+A)=0+A$ implies $a+A=0+A$ or $b+A=0+A$

$\iff$ $ab+A=0+A$ implies $a\in A$ or $b\in A$

$\iff$ $ab\in A$ implies $a\in A$ or $b\in A$

$\iff$ $A=$ prime

2. ($\implies$) Suppose $R\,/\,A$ = field. Let $B\supset A$ be an ideal ($B\neq A$). Then $\exists b\in B$ such that $b\notin A$

$\implies$ $b+A\neq 0+A$ in $R\,/\,A$

$\implies$ $\exists c$ such that $(b+A)(c+A)=bc+A=1+A$ in $R\,/\,A$

$\implies$ $bc-1=a\in A$

$\implies$ $bc-a\in B \implies B=R \implies A=$ maximal

($\impliedby$) Conversely, suppose $A=$ maximal.

For any $b+A\neq 0+A\in R\,/\,A$ (i.e. $b\notin A$)

Consider $B=\{rb+a\mid r\in R, a\in A\}$ (check B is an ideal and $B\supset A,\ B\neq A$)

$\implies$ $B=R \implies \exists r\in A$ such that $rb+a=1$ for some $a\in A$

$\implies$ $(r+A)(b+A)=(1+A)$

$\implies (b + A)$ is invertible in $R \,/\, A$

$\implies R \,/\, A = \text{field}$

$\square$

15 Ring Homomorphisms

Definition 15.1 (Ring Homomorphism). A ring homomorphism $\phi : R \to S$ is a map that preserves the two operations:

1. $\phi(a + b) = \phi(a) + \phi(b)$
2. $\phi(ab) = \phi(a)\phi(b)$

Examples.

- $\phi : \mathbb{Z} \to \mathbb{Z}_n$, $k \mapsto k \bmod n$
- $\phi : \mathbb{C} \to \mathbb{C}$, $a + bi \mapsto a - bi$ (isomorphism)
- $\phi : \mathbb{R}[x] \to \mathbb{R}$, $f(x) \mapsto f(a)$ where $a \in \mathbb{R}$ Check that $\phi(f(x) + g(x)) = \phi(f(x)) + \phi(g(x))$ and $\phi(f(x)g(x)) = \phi(f(x))\phi(g(x))$

Example 15.1. $\phi : \mathbb{Z}_4 \to \mathbb{Z}_{10},\ x \mapsto 5x$

$$\begin{aligned}
(!!!) \quad \phi(x+y) &= 5(x + y \bmod 4) \bmod 10 \\
&= 5x + 5y = \phi(x) + \phi(y) \\
(\bigstar) \quad \phi(xy) &= 5xy \bmod 10 \\
&= 5x5y \bmod 10 = \phi(x)\phi(y)
\end{aligned}$$

Example 15.2. Determine all ring homomorphisms $\mathbb{Z}_{12} \mapsto \mathbb{Z}_{30}$

Group homomorphisms: $x \mapsto ax$ where $|a| \mid \gcd(12, 30) = 6$ (i.e., $|a| = 1,\ 2,\ 3,\ \text{or } 6$)

$\implies a = 0, 15, 10, 20, 5, 25$

Ring homomorphisms: $a = \phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1) = a^2 \bmod 30$

$\implies a \equiv a^2 \bmod 30$

$\implies a \neq 5,\ a \neq 20\ (\phi(xy) = axy = a^2xy = axay = \phi(x)\phi(y) \bmod 30)$

Thus there are 4 ring homomorphisms:

$$\begin{aligned}
x &\mapsto 0x \bmod 30 \\
x &\mapsto 15x \bmod 30 \\
x &\mapsto 10x \bmod 30 \\
x &\mapsto 25x \bmod 30
\end{aligned}$$

Example 15.3. R commutative ring, $\text{char}(R) = p > 0$

$\phi : R \to R$, $x \mapsto x^p$

$$\phi(xy) = (xy)^p = x^p y^p = \phi(x)\phi(y)$$

$$\phi(x+y) = (x+y)^p = x^p + y^p + \underbrace{\sum_{i=1}^{p-1} \binom{p}{i} x^i y^{p-i}}_{p \text{ divides } \binom{p}{i}} = x^p + y^p = \phi(x) + \phi(y)$$

15.1 Properties of Ring Homomorphisms

Theorem 15.1 (Properties of Ring Homomorphisms)**.** Let $\phi : R \to S$ be a ring homomorphism. Then

1. $\phi(nr) = n\phi(r)$, $\phi(r^n) = \phi(r)^n \quad \forall r \in R, n \in \mathbb{Z}_{>0}$
2. A is a subring of $R \implies \phi(A) = \{\phi(a) \mid a \in A\}$ is a subring of S
3. A ideal and ϕ onto $S \implies \phi(A)$ ideal of S
4. $\phi^{-1}(B) = \{r \in R \mid \phi(r) \in B\}$ is an ideal of R
5. If R commutative, then $\phi(R)$ commutative
6. If R has a unity 1, $S \neq \{0\}$, and ϕ is onto, then $\phi(1)$ is the unity of S.