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. $n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$ 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 <u>characteristic</u> of a ring R is the least positive integer $\mathrm{char}(R) = n$ 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. $\mathrm{char}(\mathbb{Z}) = 0,\ \mathrm{char}(\mathbb{Z}_n) = n,\ \mathrm{char}(\mathbb{Z}_2) = 2$

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

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 $\mathrm{char}(R)$ is either 0 or prime.

Proof. Suppose $\mathrm{char}(R) = n \geq 0 \iff$ 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 $\mathrm{char}(1) = n$, 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) <u>ideal</u> 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 <u>proper ideal</u> 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 and ar are in I for all $a \in I$ and for all $r \in R$

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

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

$\square$

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,

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

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

14.3 Prime Ideals and Maximal Ideals

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 $ab\in P$, then $a\in P$ or $b\in P$.

A maximal ideal of a commutative ring R is a proper ideal A of R such that if B is an ideal of R and $A\subseteq B\subseteq R$, then $B=A$ or $B=R$.

Example 14.12. $n\mathbb{Z}\subseteq\mathbb{Z}$ is a prime ideal $\iff$ $n=0$ or n prime.

Note. $n=0$, if $a,b\in\mathbb{Z}$ such that $ab=0$, then $a=0$ or $b=0$ ✓

n prime, if $a,b\in\mathbb{Z}$, $n\mid ab$ then $n\mid a$ or $n\mid b$ ✓

Moreover, $n\mathbb{Z}\subseteq\mathbb{Z}$ is a maximal ideal $\iff$ n prime.

Example 14.13. $\langle 2\rangle, \langle 3\rangle$ are maximal ideals of $\mathbb{Z}_{36}$. More generally, if $n = \prod_{i=1}^{r} p_i^{k_i}$, $k_i \neq 0$, then $\langle p_i\rangle$ are maximal ideals of $\mathbb{Z}_n$

Example 14.14. $\langle x^2+1\rangle$ is maximal in $\mathbb{R}[x]$

Proof. Let B be an ideal containing $\langle x^2+1\rangle$ and $B \neq \langle x^2+1\rangle$.

$\implies \exists f(x) \in B$ such that $f(x) \notin \langle x^2+1\rangle$

$\implies f(x) = (x^2+1)\cdot q(x) + r(x)$ with $r(x) \neq 0$ and $\deg r(x) < 2$.

$\implies (ax+b)\cdot x - (x^2+1)\cdot a = bx - a \in B$

$\implies (ax+b)\cdot b - (bx-a)\cdot a = bx - a \in B$

Since $r(x) \neq 0$ and $a^2+b^2 \neq 0 \implies 1 \in B \implies B = \mathbb{R}[x]$ $\square$

Example 14.15. $\langle x^2+1\rangle$ is not a prime ideal in $\mathbb{Z}_2[x]$

Note. $(x+1)(x+1) = x^2+2x+1 = x^2+1$ (since $2x \equiv 0 \pmod 2$), but $x+1 \notin \langle x^2+1\rangle$

Theorem 14.3. Let R be a commutative ring with unity, let A be an ideal of R. Then $R\,/\,A$ is an integral domain $\iff$ A is prime

Proof. $R\,/\,A =$ 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 $\square$

Theorem 14.4. Let R be a commutative ring with unity and let A be an ideal of R. Then, $R\,/\,A$ is a field $\iff$ A is a maximal ideal

Proof. ($\implies$) Suppose $R\,/\,A =$ field. Let $B \supsetneqq A$ 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 $B \supsetneqq A,\ B \neq A$)

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

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

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

$\implies R \,/\, A =$ field ☐

Corollary. Let R be a commutative ring with unity. Then all maximal ideals are prime.

Example 14.16. $4\mathbb{Z} \subseteq 2\mathbb{Z} = R$ maximal but not prime ($2 \cdot 2 = 4 \in 4\mathbb{Z}$ but $2 \notin 4\mathbb{Z}$)

Example 14.17. $\langle x \rangle$ is a prime ideal in $\mathbb{Z}[x]$. $\mathbb{Z}[x] \,/\, \langle x \rangle \cong \mathbb{Z}$ is an integral domain but not a field, so $\langle x \rangle$ is not maximal.

$$\langle x \rangle \subsetneqq \underbrace{\langle x, 2 \rangle}_{\text{maximal}} \subsetneqq \mathbb{Z}[x] \qquad \frac{\mathbb{Z}[x]}{\langle x, 2 \rangle} \cong \mathbb{Z}_2$$

Lecture 36

15 Ring Homomorphisms

15.1 Definition and Examples

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

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

A bijective ring homomorphism is called a ring isomorphism.

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 $|a| \bigm| \gcd(12, 30) = 6$ (i.e., $|a| = 1,\ 2,\ 3,$ 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:

$$x \mapsto 0x \bmod 30 \qquad x \mapsto 15x \bmod 30 \qquad x \mapsto 10x \bmod 30 \qquad x \mapsto 25x \bmod 30$$

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

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

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

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

15.2 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.
7. ϕ is an isomorphism $\iff \phi$ is onto and $\ker \phi = \{r \in \mathbb{R} \mid \phi(r) = 0\} = \{0\}$.
8. If ϕ is an isomorphism from R onto S, then ϕ^{-1} is an isomorphism from S onto R.

Lecture 37

Note. 3 is not true if ϕ is not onto; $\phi : \begin{array}{c} \mathbb{Z}_{=A=R} \to \mathbb{Z} \oplus \mathbb{Z}_{=S} \\ n \mapsto (n, n) \end{array}$

6 is not true if ϕ is not onto; $\phi : \begin{array}{c} \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z} \\ n \mapsto (n, 0) \end{array}$

Theorem 15.2. Let $\phi : R \to S$ be a ring homomorphism. Then $\ker \phi$ is an ideal of R.

Note. $x \in \ker \phi,\ y \in R;\qquad xy \in \ker \phi;\qquad \phi(xy) = \phi(x)\phi(y) = 0$ (since $\phi(x) = 0$)

Theorem 15.3. Let $\phi : R \to S$ be a ring homomorphism. Then $\begin{array}{c} R \,/\, \ker \phi \mapsto \phi(R) \\ r + \ker \phi \mapsto \phi(r) \end{array}$ is an isomorphism.

(i.e. $R \,/\, \ker \phi \cong \phi(R)$)

Theorem 15.4. Every ideal of a ring R is the kernel of a ring homomorphism.

Proof. $I \subseteq R \implies R \to R \,/\, I$ has kernel I □

Example 15.4. Let $\phi : \begin{array}{c} \mathbb{Z}[x] \to \mathbb{Z} \\ f(x) \mapsto f(0) \end{array}$ be a ring homomorphism. Then $\ker \phi = \langle x \rangle$. By Thm 15.3, $\mathbb{Z}[x] \,/\, \langle x \rangle \cong \mathbb{Z}$. Since $\mathbb{Z}$ is an integral domain but not a field, $\langle x \rangle$ is a prime but not maximal in $\mathbb{Z}[x]$.

Theorem 15.5. Let R be a ring with unity 1. The mapping $\phi : \begin{array}{c} \mathbb{Z} \to R \\ n \mapsto n \cdot 1 \end{array}$ is a ring homomorphism.

Proof.

$$\begin{array}{ccccccc} \phi(m+n) & = & \phi(m) + \phi(n) & \qquad & \phi(mn) & = & \phi(m)\phi(n) \\ \| & & \| & & \| & & \| \\ (m+n) \cdot 1 & = & m \cdot 1 + n \cdot 1 & & (mn) \cdot 1 & = & (m \cdot 1) \cdot (n \cdot 1) \end{array}$$

Note. $(m \cdot 1) = \underbrace{(1 + 1 + \cdots + 1)}_{m-\text{times}} \qquad (n \cdot 1) = \underbrace{(1 + 1 + \cdots + 1)}_{n-\text{times}}$

Remark. $\begin{array}{c} \mathbb{Z} \to R \\ 1 \mapsto r \\ n \mapsto n \cdot r \end{array}$ is a group homomorphism, but not a ring homomorphism unless $r^2 = r$.

□

Corollary 15.5.1. If R is a ring with unity an $\text{char}(R) = 0$, then R contains a subring isomorphic to $\mathbb{Z}$. If $\text{char}(R) = n > 0$, then R contains a subring isomorphic to $\mathbb{Z}_n$.

Proof. Let 1 be the unity. Consider $S = \{k \cdot 1 \mid k \in \mathbb{Z}\}$. Then $\phi : \mathbb{Z} \to S$ is a ring homomorphism $\implies \mathbb{Z} / \ker \phi \cong S$.

$\text{char}(0) : \ker \phi = 0 \implies \mathbb{Z} \cong S$

$\text{char}(n) : \ker \phi = \langle n \rangle \implies S \cong \mathbb{Z} / \langle n \rangle \cong \mathbb{Z}_n$ ☐

Corollary 15.5.2. If F is a field of $\text{char}(p) > 0$ then F contains a subfield isomorphic to $\mathbb{Z}_p$.

If F is a field of $\text{char}(0)$ then F contains a subfield isomorphic to $\mathbb{Q}$.

Proof. By Cor 15.5.1, F contains $\mathbb{Z}_p$ if $\text{char}(F) = p > 0$. If $\text{char}(F) = 0$, then Cor 15.5.1 says F contains a subring S isomorphic to $\mathbb{Z}$. In this case, let $T = \{ab^{-1} \mid a, b \in S,\ b \neq 0\}$. Then T is well defined since F is a field.

Exercise. T is a subring.

Then T is isomorphic to $\mathbb{Q}$.

Exercise. $\phi : \begin{matrix} \mathbb{Q} \to T \\ \frac{m}{n} \mapsto (m \cdot 1)(n \cdot 1)^{-1} \end{matrix}$ is an isomorphism.

☐

- Intersections of subfields of fields are also fields ($F_1 \subseteq F,\ F_2 \subseteq F,\ \underbrace{F_1 \cap F_2}_{\text{field}} \subseteq F$)
- Every field has a smallest subfield which is called the <u>prime subfield</u> of the field.

Corollary 15.5.3. $\text{char}(F) = p > 0 \implies$ the prime subfield of F is isomorphic to $\mathbb{Z}_p$

$\text{char}(F) = 0 \implies$ the prime subfield of F is isomorphic to $\mathbb{Q}$

15.3 The Field of Quotients

Theorem 15.6. Let D be an integral domain. Then there exists a field $F = Q(D)$ called the <u>field of quotients of D</u> that contains a subring isomorphic to D.

Example 15.5. $D = \mathbb{Z} \implies F = \mathbb{Q}$

Proof. Let $S = \{(a, b) \mid a, b \in D,\ \underline{b \neq 0}\}$. Define an equivalence relation on S; $(a, b) \equiv (c, d)$ if $ad = bc$.

Let F be the set of equivalence classes of S under the relation $\equiv$ and denote the equivalence class that contains

(x, y) by $\frac{x}{y}$. Define addition and multiplication on F as follows:

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

Exercise. need to verify that both operations are well defined

i.e.

$$\frac{a}{b} = \frac{a'}{b'},\ \frac{c}{d} = \frac{c'}{d'} \implies \frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'} \text{ and } \frac{ac}{bd} = \frac{a'c'}{b'd'}$$

- F is a field. Let 1 be the unity of D. Then $\frac{0}{1}$ is the additive identity and $\frac{1}{1}$ is the multiplicative identity. Additive inverse of $\frac{a}{b}$ is $\frac{-a}{b}$. Multiplicative inverse of $\frac{a}{b}$ (when $a \neq 0$) is $\frac{b}{a}$.
- The mapping $\phi : \begin{matrix} D \to F \\ x \mapsto \frac{x}{1} \end{matrix}$ is an isomorphism from D to $\phi(D)$.

$\square$

Example 15.6. $D = \mathbb{Z}[x]$

$$Q(D) = \left\{ \frac{f(x)}{g(x)} \,\middle|\, g(x) \neq 0,\ f(x) \in \mathbb{Z}[x] \right\}$$
$$\mathbb{Q}(x) = Q(\mathbb{Q}[x]) = \left\{ \frac{f(x)}{g(x)} \,\middle|\, g(x) \neq 0,\ f(x) \in \mathbb{Q}[x] \right\}$$

Note. $g(x) \neq 0 \implies$ not the zero polynomial. $g(x) = \underline{x-1}$ is allowed

Lecture 38

16 Polynomial Rings

16.1 Notation and Terminology

Definition 16.1 (Ring of Polynomials over R)**.** Let R be a commutative ring.

$$R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in R,\ n \in \mathbb{Z}_{>0}\}$$

is called the ring of polynomials over R in the indeterminate x.

Addition and multiplication are as usual.

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

If $a_n \neq 0$, then $\deg(f) = n$ and a_n is called the leading coefficient of f.

If $a_n \neq 0$ is the multiplicative identity of R, then f is called a monic polynomial.

a_0 is called the constant term of f.

If $f(x) = a_0$ then f is called a constant polynomial.

Theorem 16.1. If D is an integral domain, then $D[x]$ is an integral domain.

Proof. $f(x) = a_n x^n + \underbrace{\cdots}_{\text{lower degree}}$, $g(x) = a_m x^m + \underbrace{\cdots}_{\text{lower degree}}$, $a_n^{\neq 0}, a_m^{\neq 0} \in D$

$f(x) \cdot g(x) = (a_n \cdot a_m) x^{m+n} + \underbrace{\cdots}_{\text{lower degree}}$

D integral domain $\implies a_n \cdot a_m \neq 0 \implies f(x) \cdot g(x) \neq 0$ since the leading term is nonzero. □

Theorem 16.2 (Division Algorithm for $F[x]$)**.** Let F be a field and $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exists unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that

$$f(x) = q(x)g(x) + r(x) \quad \text{and} \quad \text{either } r(x) = 0 \text{ or } \deg r(x) < \deg g(x)$$

Pf sketch.

- May assume $g(x)$ is monic ($F =$ field).

  Say $g = x^n + a_{n-1}x^{n-1} + \cdots$

- use x^n to "cancel" terms in $f(x)$

  $f(x) = b_m x^m + \cdots$ with $m \geq n$

  $f(x) - b_m x^{m-n} \cdot g(x) =$ polynomial of degree $< m$

  Then proceed by induction on degree.

□

Example 16.1. In $\mathbb{Z}_5[x]$,

$$f(x) = 3x^4 + x^3 + 2x^2 + 1$$
$$g(x) = x^2 + 4x + 2$$

$$\begin{array}{r|l}
 & 3x^2 + 4x \\
\hline
x^2+4x+2 & 3x^4 + x^3 + 2x^2 + 0\cdot x + 1 \\
 & 3x^4 + 2x^3 + x^2 \\
\hline
 & 4x^3 + x^2 + 0\cdot x + 1 \\
 & 4x^3 + x^2 + 3x \\
\hline
 & 2x + 1
\end{array}$$

$$f(x) = \underbrace{g(x)}_{g(x)}(3x^2+4x) + \underbrace{(2x+1)}_{r(x)}$$

Corollary 16.2.1 (Remainder Theorem)**.** Let F be a field and $f(x) \in F[x]$. THen a is a zero of $f(x)$ $\iff$ $x - a$ is a factor of $f(x)$

Proof. $f(x) = (x-a)q(x) + r$ (where r is a constant)

$$\begin{aligned} a \text{ is a zero of } f &\iff f(a) = 0 \iff r = 0 \\ &\iff f(x) = (x-a)q(x) \\ &\iff (x-a) \text{ is a factor of } f \end{aligned}$$

□

Corollary 16.2.2 (Factor Theorem)**.** A polynomial of degree n over a field has at most n zeros counting multiplicity.

Pf sketch. use Cor 16.2.1 □

Example 16.2. Every polynomial in $\mathbb{C}[x]$ of deg n has exactly n zeros counting multiplicity.

Cor is not true for arbitrary polynomial rings.

Example 16.3. $x^2 + 3x + 2$ in $\mathbb{Z}_6[x]$ has <u>four</u> zeros in $\mathbb{Z}_6$ (1, 2, 4, 5).

Definition 16.2 (Principal Ideal Domain (PID))**.** A <u>principal ideal domain (PID)</u> is an integral domain R such that every ideal has the form $\langle a \rangle = \{ra \mid r \in R\}$ for some $a \in R$

Theorem 16.3. For any field F, $F[x]$ is a PID.

Proof. Let I be an ideal in $F[x]$.

Assume $I \neq \{0\} = \langle 0 \rangle$

Let g be a polynomial in I that has minimum degree.

Then $I = \langle g(x) \rangle$ by the division algorithm □

Theorem 16.4. $\mathbb{Z}$ is a PID.

Example 16.4. $\mathbb{Z}$[x] is *not* a PID. (e.g. $\langle x, 2 \rangle$ is not principal)

Lecture 38

17 Factorization of polynomials

17.1 Reducibility Tests

Definition 17.1 (Irreducible/Reducible Polynomial)**.** Let D be an integral domain. A polynomial $f(x) \in D[x]$ that is neither 0 nor a unit in $D[x]$ is said to be irreducible over D if whenever $f(x) = g(x)h(x)$, then $g(x)$ or $h(x)$ is a unit in $D[x]$. A nonzero, nonunit element of $D[x]$ that is *not* irreducible is said to be reducible.

Example 17.1.

$$\begin{aligned} f(x) &= 2x^2 + 4 \\ &= 2 \cdot (x^2 + 2) \\ &= 2(x + \sqrt{-2})(x - \sqrt{-2}) \end{aligned}$$

Reducible over $\mathbb{Z}$, $\mathbb{C}$. Irreducible over $\mathbb{Q}$, $\mathbb{R}$.

Example 17.2. $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{R}$.

Theorem 17.1 (Reducibility Test for Degrees 2 and 3)**.** Let F be a field and $f(x) \in F[x]$ such that $\deg f = 2$ or 3. Then $f(x)$ is reducible over $F \iff f(x)$ has a zero in F.

Pf sketch. If $f(x) = g(x)h(x)$ then $\deg g(x) + \deg h(x) = \deg f(x) = 2$ or 3. So $g(x)$ or $h(x)$ has a degree of 1 (if $\deg g(x) = 0$ or $\deg h(x) = 0$ then $g(x)$ or $h(x)$ is a unit).

$$\begin{aligned} \deg 1 &\implies ax + b, \quad a, b \in F \\ &\implies a(x + \frac{b}{a}) \\ &\implies -\frac{b}{a} \text{ is a zero of } f(x) \end{aligned}$$

□

Example 17.3. $x^2 + 1$ is irreducible over $\mathbb{Z}_3 \quad \Longleftarrow \quad (0^2 + 1 = 1,\ 1^2 + 1 = 2,\ 2^2 + 1 = 5 = 2 \text{ in } \mathbb{Z}_3)$

$x^2 + 1$ is reducible over $\mathbb{Z}_5 \quad \Longleftarrow \quad (x^2 + 1 = (x - 2)(x - 3) \text{ in } \mathbb{Z}_5[x])$

Exercise. Prove Example 17.3

Example 17.4. $x^4 + 2x^2 + 1 = (x^2 + 1)^2$ is reducible over $\mathbb{Q}$ (or $\mathbb{R}$) in $\mathbb{Q}[x]$ (or $\mathbb{R}[x]$) but $x^4 + 2x^2 + 1$ has no zeros in $\mathbb{Q}$ (or in $\mathbb{R}$)

Definition 17.2 (Content of a Polynomial, Primitive Polynomial)**.** The content of a nonzero polynomial

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

is the greatest common divisor of $a_n, a_{n-1}, \ldots, a_0$. A primitive polynomials is an element in $\mathbb{Z}[x]$ with content 1.

Lemma 17.1 (Gauss's Lemma)**.** The product of two primitive polynomials in $\mathbb{Z}[x]$ is primitive.

Proof. Assume $f(x), g(x)$ are primitive, and suppose $f(x)g(x)$ is not primitive. Let p be a prime divisor of the content of $f(x)g(x)$. Consider the ring homomorphism from $\phi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$. Let $\overline{f(x)g(x)}$ be the image of $f(x)g(x)$ in $\mathbb{Z}_p[x] \implies \overline{f(x)g(x)} = \overline{f(x)g(x)}$

Note. In other words, $\overline{f(x)}$ is the polynomial in $\mathbb{Z}[x]$ obtained by reducing the coefficients of $f(x)$ modulo p.

Since $p \mid$ content of $f(x)g(x) \implies \overline{f(x)g(x)} = 0$ in $\mathbb{Z}_p[x]$
$\implies \overline{f(x)} = 0$ or $\overline{g(x)} = 0$ because $\mathbb{Z}_p[x]$ is an integral domain.
$\implies f(x)$ or $g(x)$ is not primitive. ($\Rightarrow\Leftarrow$) $\square$

Theorem 17.2. Let $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is reducible over $\mathbb{Q}$, it is reducible over $\mathbb{Z}$.

Proof. Assume $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{Q}[x]$. Let a and b be the LCM of denominators of coefficients of $g(x)$ and $h(x)$ respectively. Then $(ab)f(x) = abg(x)h(x) = (ag(x))(bh(x))$. Let c_1 and c_2 be the content of $ag(x)$ and $bh(x)$ respectively. Then $ag(x) = c_1\hat{g}(x)$ and $bh(x) = c_2\hat{h}(x)$ where $\hat{g}(x)$ and $\hat{h}(x)$ are primitive in $\mathbb{Z}[x]$. Let d be the content of f (i.e. $f(x) = d\hat{f}(x)$ where $\hat{f}(x) \in \mathbb{Z}[x]$ is primitive.) Then $(abd)\hat{f}(x) = (c_1c_2)\hat{g}(x)\hat{h}(x) \in \mathbb{Z}[x]$. By Gauss' lemma, $\hat{g}(x)\hat{h}(x)$ is primitive in $\mathbb{Z}[x]$
$\implies abd = c_1c_2 \implies \hat{f}(x) = \hat{g}(x)\hat{h}(x)$
$\implies f(x) = d\hat{f}(x) = (d\hat{g}(x)) \cdot \hat{h}(x)$
$\implies f(x)$ is reducible over $\mathbb{Z}$ (since $d\hat{g}(x), \hat{h}(x) \in \mathbb{Z}[x]$). $\square$

Example 17.5. $f(x) = 6x^2 + x - 2 = \underbrace{(3x - \frac{3}{2})}_{g(x)}\underbrace{(2x + \frac{4}{3})}_{h(x)}$

$d = 1,\ a = 2,\ b = 3,\ c_1 = 3,\ c_2 = 2 \implies f(x) = (2x - 1)(3x + 2)$

FINISH EXAMPLE (NOTES-38)

Theorem 17.3. Let p be prime and $f(x) \in \mathbb{Z}[x]$ such that $\deg f \geq 1$. $\overline{f(x)}$ reducing coeff of $f(x)$ modulo p.

If $\overline{f(x)}$ is irreducible over $\mathbb{Z}_p$ and $\deg \overline{f(x)} = \deg f(x)$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Remark. $f(x) = 21x^3 - 3x^2 + 2x + 9$ work over $\mathbb{Z}_2$

$\overline{f(x)} = x^3 + x^2 + 1$ has no zero in $\mathbb{Z}_2 \implies$ irridducible

Lecture 40