
[1]

MATH 323 Rings and Modules

Wucheng Zhang

http://blogs.ubc.ca/wucheng/

[1]This image is from http://cen.xraycrystals.org/essay-on-the-future-of-crystallography.html

Contents

Lecture 1	Lecture 2	Lecture 3	Lecture 4
Lecture 5	Lecture 6	Lecture 7	Lecture 8
Lecture 9	Lecture 10	Lecture 11	Lecture 12
Lecture 13	Lecture 14	Lecture 15	Lecture 16
Lecture 17	Lecture 18	Lecture 19	Lecture 20
Lecture 21	Lecture 22	Lecture 23	Lecture 24
Lecture 25	Lecture 26	Lecture 27	Lecture 28
Lecture 29	Lecture 30	Lecture 31	

Lecture 1 Jan 7

Topic: Introduction, Number Theory (Review), Definition of Rings, Invertible Elements

Introduction Rings and modules could be related many other fields.

1. Representation theory (algebraic, analytic).
2. Algebraic number theory (e.g. what is the difference between π/e and $\sqrt{2}$? $\sqrt{2}$ is related to $\mathbb{Q}[x]/(x^2-2)$).
3. Algebraic geometry (e.g. What is the difference between $y = x^2$ and $y^2 = x^3$, i.e. where does the singularity in $y^2 = x^3$ come from? $y = x^2$ is related to $\mathbb{R}[x, y]/(y - x^2)$ while $y^2 = x^3$ is related to $\mathbb{R}[x, y]/(y^2 - x^3)$).

Number Theory Review

1. $\mathbb{N}$ is the set of natural numbers where $0 \in \mathbb{N}$.
2. $\mathbb{Z}$ is the set of integers.
3. **Well ordering principle**: A nonempty subset of $\mathbb{Z}$ which is bounded below/above has a smallest/largest element. (*Note*: This is not true in $\mathbb{R}$, i.e $(0, 1]$).
4. **Divisibility**: Let $a, b \in \mathbb{Z}$, $a \neq 0$, a divide b and we write $a|b$ when there exists $c \in \mathbb{Z}$ such that $b = ac$.
5. **Greatest common divisor**: Let $a, b \in \mathbb{Z}$ and $(a, b) \neq (0, 0)$, $\gcd(a, b) = \max\{d \in \mathbb{Z} \big| d|a \text{ and } d|b\} \geq 1$.
6. **Coprime**: If $\gcd(a, b) = 1$, then a, b are coprime.
7. **Least common multiple**: Let $a, b \in \mathbb{Z}$ and $(a, b) \neq (0, 0)$, $\operatorname{lcm}(a, b) = \min\{m \in \mathbb{N} \big| a|m \text{ and } b|m\}$.
8. $\mathbb{Z}$ is a unique factorization domain. This means, for any $x \in \mathbb{Z}$,

$$x = \pm \prod p^{n_p}$$

   where p is prime, $n_p \in \mathbb{N}$ and $n_p = 0$ except for finite p.
   Consequence: Let $a, b \in \mathbb{Z}$ and $a = \pm \prod p^{n_p}$, $b = \pm \prod p^{m_p}$. Then $\gcd(a, b) = \prod p^{\min(n_p, m_p)}$ and $\operatorname{lcm}(a, b) = \prod p^{\max(n_p, m_p)}$. Then $\gcd(a, b) \times \operatorname{lcm}(a, b) = |ab|$. And for any $d \in \mathbb{Z}$, if $d|a$ and $d|b$, we would have $d| \gcd(a, b)$.

9. **Division algorithm**: $a, b \in \mathbb{Z}$, $b > 0$, there exists unique $(q, r) \in \mathbb{Z}^2$ such that $a = bq+r$ where $0 \leq r < r$. We call q as quotient and r as remainder.
   Proof. (!!Sketch!!) Let $S = \{a - bk | k \in \mathbb{Z}\} \cap \mathbb{N}$. It is clear that $S \neq$ and S is bounded below. Then let $r = \min(S)$ by well ordering principle. There exists k such that $a - bk = r$, call it q. Then check $0 \leq r \leq b$ and check a pair (q, r) as in the theorem is unique.

Formalism of $\mathbb{Z}$ as a group

1. $(\mathbb{Z}, +)$ is a group.
2. The subgroups of $(\mathbb{Z}, +)$ are of the form $a\mathbb{Z}$, where $a \in \mathbb{N}$.
   Proof. (Sketch!!) If $H = \{0\}$, $H = 0\mathbb{Z}$. Otherwise, $H \cap (\mathbb{N}\backslash\{0\}) \neq \emptyset$. Let $a = \min(H \cap (\mathbb{N}\backslash\{0\}))$. Using division algorithm, prove $H = a\mathbb{Z}$.
3. Let $a, b \in \mathbb{Z}$ and $(a, b) \neq (0, 0)$, $a\mathbb{Z} + b\mathbb{Z} := \{au + bv | u, v \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$. In particular, $a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\mathbb{Z}$.
   Proof. (Sketch!!) First prove it is a subgroup. Then there exists $d \in \mathbb{N}$, $d \geq 1$ such that $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Let $D = \gcd(a, b)$. First by $a\mathbb{Z} \subset d\mathbb{Z}$ and $b\mathbb{Z} \subset d\mathbb{Z}$, we know $d|a$ and $d|b$ and then $d|D$. Second, since $d \in d\mathbb{Z}$, there exists $u_0, v_0 \in \mathbb{Z}$, $d = au_0 + bv_0$. Then $D|d$. Then $d = D$.

   Remark. It means that there exists $u, v \in \mathbb{Z}$ such that $\gcd(a, b) = au + bv$.
   Exercise. Find $u, v \in \mathbb{Z}$ for 25 and 7 such that $25u + 7v = \gcd(25, 7)$. We need to find $25u + 7v = 1$. Then $u = \dfrac{1 - 7v}{25}$. One solution is $v = -7$ and $u = 2$.

Integers mod n for $n \in \mathbb{N}$, $n \geq 1$

1. **Relation on** $\mathbb{Z}$: $x \sim y$ when $n | x - y$. It is a equivalence relation. We denote the set of classes $\mathbb{Z}/\sim = \mathbb{Z}/n\mathbb{Z} = \{[x], x \in \mathbb{Z}\}$ where $[x] = \{y \in \mathbb{Z} | y \sim x\}$.
2. **Notation**: Instead of $x \sim y$, we write $x \equiv y \mod n$ and $[x] = \{y \in \mathbb{Z} | y \equiv x \mod n\} = x + n\mathbb{Z}$. Then by division algorithm, $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\} = \{\mathbb{Z}, 1+\mathbb{Z}, \ldots, (n-1) + \mathbb{Z}\}$.
3. **Operators**: $[x] \oplus [y] := [x + y]$ and $[x] \otimes [y] := [x \times y]$.
   Check. It makes sense since $x' \in [x], y' \in [y]$ then $[x'+y'] = [x+y]$ and $[x' \times y'] = [x \times y]$. (1) Namely, $x \equiv x' \mod n$ and $y \equiv y' \mod n$ then $x + y \equiv x' + y' \mod n$. (2) Namely, $x \equiv x' \mod n$ and $y \equiv y' \mod n$ then $x \times y = x' \times y'$ since $x'y' - xy = x'(y' - y) + y(x' - x)$.
4. $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ is a group with identity element $[0]$.
   Remark. $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ is not a group since $[1]$ is the identity and $[0]$ does not have an inverse.

Rings

Definition 1. Let R be a set equipped with 2 operations $+$ and $\times$. $(R, +, \times)$ is called a ring if

- $(R, +)$ is an abelian group.
- $\times$ is an associative operation.
- $\times$ is distributive with $+$, $r \times (s+t) = (r \times s) + (r \times t)$ and $(s+t) \times r = (s \times r) + (t \times r)$.

Note. The identity element of $+$ is called 0_R or 0.

Definition 2. A ring $(R, +, \times)$ is called commutative when $\times$ is commutative. A ring $(R, +, \times)$ is called unitary if $\times$ has an identity element called 1_R or 1, i.e. $1_R \times r = r \times 1_R = r$ for any $r \in R$.
Note. Our rings will be unitary.

Example 1. Rings.

1. $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ and $(\mathbb{C}, +, \times)$.
2. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.
3. Let $\mathcal{F} = \{f : \mathbb{R} \to \mathbb{R}\}$, $(f+g)(x) = f(x) + g(x)$, $(fg)(x) = f(x)g(x)$. Then $(\mathcal{F}, +, \times)$ is a ring. But $(\mathcal{F}, +, \circ)$ is not a ring where $f \circ g(x) = f(g(x))$.
4. $(M_{n\times n}(\mathbb{R}), +, \times)$ is not a commutative ring.

Definition 3. Let $(R, +, \times)$ be unitary ring, $r \in R$ is called invertible (or the unit of the ring) if there exits $r' \in R$ such that $r \times r' = r' \times r = 1_R$. The set of invertible elements is denoted by $R^\times$.

Example 2. Invertible elements.

1. $\mathbb{Q}^\times = \mathbb{Q}\backslash\{0\}$.
2. $\mathbb{R}^\times = \mathbb{R}\backslash\{0\}$.
3. $\mathbb{Z}^\times = \{\pm 1\}$.
4. $(M_{n\times n}(\mathbb{R}))^\times = GL_n(\mathbb{R})$.

Lecture 2

Jan 8

Topic: More on Invertible Elements, Integral Domain, Field, Subring, Homomorphism

Invertible Elements/Units

Proposition 1. $(R^\times, \times)$ is a group.
Proof.

Example 3. What is $(\mathbb{Z}/n\mathbb{Z})^\times$? First try $(\mathbb{Z}/4\mathbb{Z})^\times = \{\bar{1}, \bar{3}\}$. We want to generalize that $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{x} | \gcd(x, n) = 1\}$.
Key: $\gcd(n, x)\mathbb{Z} = n\mathbb{Z} + x\mathbb{Z}$. In particular $\gcd(n, x) = 1$, then there exists $u, v \in \mathbb{Z}$ such that $1 = nu + xv$. Vice versa if there exists $u, v \in \mathbb{Z}$ such that $1 = mu + xv$ then $1 \in n\mathbb{Z} + x\mathbb{Z}$, namely $\mathbb{Z} = n\mathbb{Z}+x\mathbb{Z}$. This is just **B'ezont Theorem**: $\gcd(x, n) = 1 \iff \exists u, v \in \mathbb{Z}, \text{ s.t. } 1 = xu + nv$.
Proof. First, $\bar{x} \in (\mathbb{Z}/n\mathbb{Z})^\times$, there exists $\bar{y} \in \mathbb{Z}/n\mathbb{Z}$ such that $\bar{x}\bar{y} = 1$. Then $xy - 1 \in n\mathbb{Z}$, there exists $u \in \mathbb{Z}$ such that $xy - 1 = nu$. Then $1 = un + (-y)x$. So $\gcd(n, x) = 1$. Therefore $(\mathbb{Z}/n\mathbb{Z})^\times \subset \{\bar{x} | \gcd(x, n) = 1\}$. Second, if $\gcd(x, n) = 1$, by B'ezont theorem, there exists $u, v \in \mathbb{Z}$ such that $1 = xu + nv$. Then $\bar{1} = \bar{x}\bar{u}$. so $\bar{x}$ is invertible with inverse $\bar{u}$.
Remark 1. We define $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$, called Euler ϕ function.
Remark 2. If p is prime number, $(\mathbb{Z}/p\mathbb{Z})^\times = \{\bar{1}, \ldots, \overline{p-1}\}$ and $\phi(p) = p - 1$. So $\bar{x}^{p-1} = \bar{1}$. So if $p \not| x$, we have $x^{p-1} \equiv 1 \mod p$. This is equivalent to say $x^p \equiv x \mod p$ for any x. This is called Fermat little theorem.

Integral Domain & Field

Definition 4. Let $(P, +, \times)$ be a unitary, commutative ring.

1. R us an integral domain if it has no nonzero divisor, i.e., for any $x, y \in R$, $xy = 0_R$ would imply $x = 0_R$ or $y = 0_R$.
2. R is a field if $R^\times = R \backslash \{0_R\}$.

Example 4. Integral Domain & Field

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ are integral domains.
2. $\mathbb{Z}/4\mathbb{Z}$ is not an integral domain since $\bar{2} \times \bar{2} = \bar{4} = \bar{0}$.
3. $\mathbb{Q}$ and $\mathbb{R}$ are fields.
4. $\mathbb{Z}$ is not a field since $\mathbb{Z}^\times = \{\pm 1\}$.
5. $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.

Proposition 2. A field is an integral domain.
Proof. Let $(R, +, \times)$ be a field. Let $x, y \in R$ such that $xy = 0_R$. If $x \neq 0_R$ then $x \in R\backslash\{0\} = R^\times$, so there exists x' such that $x'x = 1_R$. Then $y = x'xy = x'0_R = 0_R$. Then R is a integral domain.
Remark. If $(R, +, \times)$ is not commutative but $R^\times = R\backslash\{0\}$ then R is a division ring.

Example 5. If R is an integral domain such that R is a finite set, R is a field.
Proof. Let R be an integral domain and suppose R is finite. We want to show R is a field. Let $r \in R\backslash\{0\}$. Consider $m_r : R \to R$ denoted by $x \mapsto xr$. This is a homomorphism on group. Let $x \in \ker m_r$. This means $xr = 0_r$ and then $x = 0_R$ because R is an integral domain. So m_r is injective. And $|R| < \infty$ so m_r is surjective. So there exists $x \in R$ such that $m_r(x) = 1_R$, namely $xr = 1_R$.

Subring

Definition 5. $(R, +, \times)$ is a unitary ring and $S \subset R$. Then $(S, +, \times)$ is a (unitary) subring of R if

1. $(S, +)$ is a subgroup of $(R, +)$.
2. S is closed under $\times$.
3. $1_R \in S$.

Example 6. Subrings.

1. $\mathbb{Q}$ is a subring of $\mathbb{R}$.
2. $\mathbb{Z}$ is a subring of $\mathbb{Q}$.
3. $M_2(\mathbb{Z})$ is a subring of $M_2(\mathbb{R})$.
4. $\mathcal{F}^{\text{cont}}$ is a subring of $\mathcal{F}$.

Homomorphism

Definition 6. Let $(R, +, \times)$ and $(S, +, \times)$ be two unitary rings. Then $f : R \to S$ is a homomorphism of unitary rings if

1. $f : (R, +) \to (S, +)$ is a homomorphism of groups.
2. $f(x \times y) = f(x) \times f(y)$ for any $x, y \in R$.
3. $f(1_R) = 1_S$.

Note 1. We say f is an isomorphism of rings if f is surjective. !!Check!! that the inverse map $f^{-1} : S \to R$ is a homomorphism of rings.
Note 2. We define the kernel $\text{Ker} f = f^{-1}\{0_S\}$ (preimage). Then f is injective if and only if $\ker f = \{0_R\}$. Notice $1_R \notin \ker f$.
Note 3. Image of f, $f(R)$ is a subring of S.

Example 7. Homomorphisms of rings.

1. $Id : \mathbb{Z} \to \mathbb{R}$ denoted by $x \mapsto x$ is a homomorphism of rings. The kernel is $\{0\}$.
2. $f_s : \mathcal{F} \to \mathbb{R}$ denote by $\varphi \mapsto \varphi(s)$ is a homomorphism of rings. For example $f_s(\tilde{1}) = 1_R$. The image is $\mathbb{R}$ and the kernel is $\{\varphi : \mathbb{R} \to \mathbb{R} | \varphi(s) = 0\}$.
3. Let R_1, R_2 to be two rings. Consider the product $R_1 \times R_2 = \{(r_1, r_2) | r_1 \in R_1, r_2 \in R_2\}$. $R_1 \times R_2$ has a structure of ring addition and multiplication coordinate by coordinate. Identity element of $R_1 \times R_2$ is $(1_{R_1}, 1_{R_2})$. Then $f_1 : (R_1, R_2) \to R_1$ denoted by $(r_1, r_2) \mapsto r_1$ is a ring homomorphism. And $f_2 : R_1 \to (R_1, R_2)$ denoted by $r_1 \mapsto (r_1, 1_{R_2})$ is not a ring homomorphism since it does not preserve addition.
4. $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ denoted by $x \mapsto x \mod n$ is a homomorphism of rings.

Lecture 3 Jan 14

Topic: More on Homorphism; Field of Fraction of an Integral Domain; Ideals of a Unitary Ring

An example on Homomorphism

Example 8. Let R be a unitary ring with $1_R \in R$ and let $e \in R$ to be idempotent, i.e. $e \times e = e$. Check that $eRe = \{exe, x \in R\}$ is a ring: $exe + eye = e(x+y)e$ and $(exe)(eye) = e(xey)e$. It is is a unitary ring with unit e. eRe is a ring contained in R but in general they don't have the same unit. Then eRe is not a subring of R.

Remark. $(1_R - e)^2 = (1_R - e)(1_R - e) = 1_R - e - e + ee = 1_R - e$. So likewise $(1_R - e)R(1_R - e)$ is also a ring.

Exercise. Study the map $f : R \to eRe \times (1-e)R(1-e)$ by $r \mapsto (ere, (1-e)r(1-e))$. It is an isomorphism of rings?

Field of Fraction of an Integral Domain

Definition 7. Let R be an integral domain. On $R \times (R \backslash \{0\})$ define the notation $(x, y) \sim (x', y')$ when $xy' = yx'$. Then

1. We could check it is equivalence relation.
2. Change the notation: Let $(x, y) \in R \times (R \backslash \{0\})$. Its equivalence class $[(x, y)]$ is denoted by $\frac{x}{y}$ and the set of all these equivalence class denoted by $\text{frac}(R) = R \times (R \backslash \{0\}) / \sim$.
3. Equip frac(R) with a structure of ring. We define $\frac{x}{y} \oplus \frac{x'}{y'} := \frac{xy' + yx'}{yy'}$ and $\frac{x}{y} \otimes \frac{x'}{y'} = \frac{xx'}{yy'}$. Then we have to
   (a) Show that these operations are well defined. Let $(x_1, y_1) \sim (x_1', y_1')$ and $(x_2, y_2) \sim (x_2', y_2')$. We need to check $y_1y_2, y_1'y_2' \in R \backslash \{0\}$, $(x_1y_2 + x_2y_1, y_1y_2) \sim (x_1'y_2' + x_2'y_1', y_1'y_2')$ and $(x_1x_2, y_1y_2) \sim (x_1'x_2', y_1'y_2')$.
   (b) $(\text{frac}(R), \oplus)$ is a commutative group.
   (c) $\otimes$ is distributive with respect to $\oplus$.
   (d) $\otimes$ is associative.

   Then frac(R) is a ring. In fact, it is a unitary ring with $\frac{1_R}{1_R} (= \frac{x}{x}$ for any $x \in R \backslash \{0\})$.

   Remark. Neutral element in frac(R) is $\frac{0_R}{1_R} (= \frac{0_R}{x}$ for any $x \in R \backslash \{0\})$. Let $\frac{x}{y} \notin \text{frac}(R) \backslash \{\frac{0_R}{1_R}\}$, it means that $x \neq 0_R$. Can consider $[(x, y)] = \frac{y}{x}$, we have $\frac{x}{y}\frac{y}{x} = \frac{xy}{xy} = \frac{1_R}{1_R}$. So $\frac{x}{y}$ is invertible and frac(R) is a field.

4. Consider $\varphi : R \to \text{frac}(R)$ such that $x \mapsto [(x, 1_R)] = \frac{x}{1_R}$. This is a homomorphism of rings. This is injective because $\ker\varphi = \{x \in R | \frac{x}{1_R} = \frac{0_R}{1_R}\} = \{x \in R | x1_R = 0_R 1_R = 0_R\} = \{0_R\}$.

5. *Note.* In fact frac(R) is the smallest field containing R.

Example 9. (Field of Fraction)

1. $\text{frac}(\mathbb{Z}) := \mathbb{Q}$.

2. Let k be a field, $k[x] = \{\sum_{i=0}^{n} a_i x^i | n \in \mathbb{N}, a_i \in k\}$ to be the set of polynomials in the variable x with coefficient in k. Then $\text{frac}(k[x]) := k(x) = \{\frac{P}{Q} | P, Q \in k[x], Q \neq 0\}$.

Ideals of a unitary ring

Definition 8. Let $I \subset R$. It is a left (respectively right) ideal of R if

1. $(I, +)$ is a subgroup of $(R, +)$.

2. $r \times I \subset I$ for any $r \in R$, namely $r \times x \in I$ for any $r \in R$ and $x \in I$. (respectively $I \times r \subset I$).

Definition 9. We say $I \subset R$ is a two sided ideal of R if it is a left ideal and a right ideal. But if R is commutative, we just say ideal (left=right=two-sided).

Example 10. (left/right/two-sided ideals)

1. $\{0_R\}$ and R are 2-sided ideals of R.

2. If k is a field, then the ideals of k is 0_k and k.
   Proof. Let $I \subset k$ to be an ideal and $I \neq \{0_k\}$. Let $x \in I \setminus \{0_k\}$. It is invertible then $1_k = \underbrace{x^{-1}}_{\in k} \times \underbrace{x}_{\in I} \in I$. Not let $y \in k$, $y = \underbrace{y}_{\in k} \times \underbrace{1_k}_{\in I} \in I$. Then $k \subset I$ and $k = I$.

3. Let $f : R \to S$ to be the ring homomorphism. Let J to be a (left/right/two-sided) ideal of S. Then $f^{-1}(J)$ is a (left/right/two-sided) ideal of R. This is because $x \in f^{-1}(J), y \in R$ then $f(xy) = f(x)f(y) \in J$. Then $(f^{-1}(J), +)$ is a subgroup of R because f is a homomorphism of groups for $+$.

4. $f : R \to S$ is homomorphism of rings. Then $\ker f$ is a two-sided ideal.

5. (Consequence to 4) Let $f : k \to R$ to be the homomorphism of unitary rights. $f(1_k) = 1_R$ then f is not the zero map (does not send entire k to 0_R, namely $\ker f \neq k$). So $\ker f = \{0_R\}$ and f is injective. So k identifies as a subring of R.

6. Ideals of $\mathbb{Z}$ are all the $n\mathbb{Z}$ for $n \in \mathbb{N}$.

7. Let $f : R \to S$ to be the homomorphism of unitary rings. Let I to be the ideal of R. $f(I)$ is not necessary an ideal. *Note.* $f(I)$ is an ideal if f is isomorphism.

Proposition 3. If I and J are (left/right/two-sided) ideals of R, $I \cap J$ is an (left/right/two-sided) ideal of R.
Proof. $I \cup J$ is a subgroup of R. For any $r \in R$, $x \in I \cup J$, (for example) $xr \in I$ and $xr \in J$ and then $xr \in I \cup J$.

Definition 10. If $X \subset R$, we call

$$(X) = \bigcap_{X \subset J,\, J \text{(left/right/two-sided) ideal}} J$$

is the (left/right/two-sided) ideal generated by X.
Note. For any ideal I of R, if $X \subset I$, $(X) \subset I$.

Example 11. $X = \{a\}$ where $a \in R$, the left ideal generated by a is $(a) = Ra = \{ra, r \in R\}$.

Lecture 4 Jan 16

Topic: Quotient Ring; Isomorphism theorem

Quotient Ring

Definition 11. Let R be a ring, $I, J \subset R$ are left/right/two-sided ideals. Then we define $I + J = \{x + y | x \in I, y \in J\}$ and $IJ = \left\{ \sum_{i=1}^{n} x_i y_i \middle| n \geq 1, x_i \in I, y_i \in J \right\}$. *Note*: $I + J$ and IJ are still left/right/two-sided ideals.

Definition 12. Let $(R, +, \times)$ be a unitary ring. Let I be an **two-sided** ideal. Define a relation on R such that $x \sim y$ when $x - y \in I$ (check by $(I, +)$ is an abelian group). Then let $R/I = R/\sim = \{x + I | x \in R\}$. We want to define a structure of rings on R/I such that the canonical map $\pi : R \to R/I$ by $x \to x + I$ is a homomorphism of unitary ring. Let $x, y \in R$, check that: $(x + I) \oplus (y + I) = \pi(x) \oplus \pi(y) = \pi(x + y) = (x + y) + I$ and $(x + I) \otimes (y + I) = \pi(x) \otimes \pi(y) = \pi(xy) = (xy) + I$. So that's how we define $\oplus$ and $\otimes$ on R/I.

Remark 1. Is this really a well defined structure of ring on R/I?

1. Check: Well defined. Let $x, x', y, y' \in R$ such that $x \sim x'$ and $y \sim y'$. We know

$$(x' + y') - (x + y) = \underbrace{(x - x')}_{\in I} + \underbrace{(y - y')}_{\in I}$$

   so $x + y + I = x' + y' + I$. We also know that

$$x'y' - xy = \underbrace{\underbrace{x'}_{\in R} \underbrace{(y' - y)}_{\in I}}_{\in I} + \underbrace{\underbrace{(x' - x)}_{\in I} \underbrace{y}_{\in R}}_{\in I}$$

   so $x'y' + I = xy + I$.

2. Check that $(R/I, \oplus, \otimes)$ is a unitary ring. It is easy to see the closedness, associativity and commutativity. And $0_{R/I} = 0_R + I$ and $1_{R/I} = 1_R + I$.

3. Check that $\pi : R \to R/I$ is a homomorphism of unitary rings.

Example 12. (Examples on Quotient rings)

1. $R/\{0\} = R$.
2. $\mathbb{Z}/n\mathbb{Z}$.

3. $\mathcal{F} = \{f : \mathbb{R} \to \mathbb{R}\}$ and $I = \{f \in \mathcal{F} | f(1) = 0\}$. I is an two-sided ideal since I is the kernel of $\mathcal{F} \to \mathbb{R}$ and $f \to f(1)$. Then $\mathcal{F}/I$ is an quotient ring. It is also an $\mathbb{R}$-vector space with dimension 1. Let to be the constant function equal to 1. $[\tilde{1}] \neq 0_{\mathcal{F}/I}$ because $0_{\mathcal{F}/I} = [\tilde{0}]$ and if we had $[\tilde{1}] = [\tilde{0}]$ then $\tilde{1} - \tilde{0} \in I$ and $\tilde{1}(1) = \tilde{0}(0) + 0 = 0$. Then we want to show any element in $\mathcal{F}/I$ is $\mathbb{R}$-proportional to $[\tilde{1}]$. Let $g \in \mathcal{F}$, we claim $[g] = [\widetilde{g(1)}]$ because $g - \widetilde{g(1)} \in I$. So $[g] = g(1)[\tilde{1}]$. So $[g]$ is indeed $\mathbb{R}$-proportional to $[\tilde{1}]$ and $[\tilde{1}]$ is the basis of $\mathcal{F}/I$ as a vector space.

Remark 2. $\pi : R \to R/I$ is a homomorphism which is surjective.

We have three **corollaries**.

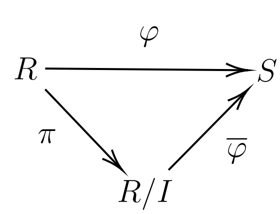
1. If J is an ideal of R/I then $\pi^{-1}(J)$ is an ideal of R containing I because $0_{R/I} \subset J$ so $I = \pi^{-1}(0_{R/I}) \subset \pi^{-1}(J)$. [cf. Example 10.3]
2. Let J be an ideal of quotients containing I, $\pi(J)$ is an ideal of R/I. [cf. Example 10.7]
3. Conclusion: For J and ideal containing I, define $J/I = \pi(J) = \{x + I | x \in J\} \subset R/I$. By 1. and 2. together, the ideals of R/I are all the J/I where J is the ideal of R containing I.
   Proof. If J is an ideal of R containing J, then $\pi(J) = J/I$ is an ideal of R/I by 2. If J is an ideal of R/I, then by 1 π^{-1} is an ideal K of R containing I. Since π surjective, $J = \pi(\pi^{-1}(J)) = \pi(K) = K/I$.

Example 13. (Examples on Remark 2.3)

1. Ideals of $\mathbb{Z}/6\mathbb{Z}$: $\mathbb{Z}/6\mathbb{Z}$, $2\mathbb{Z}/6\mathbb{Z}$, $3\mathbb{Z}/6\mathbb{Z}$ and $6\mathbb{Z}/6\mathbb{Z} = \{0\}$.
2. $\mathcal{F}$, $J = \{f \in \mathcal{F} | f(1) = 0\}$. Let $K = (x-1)\mathcal{F}$ be the set of functions generated by $x - 1$. Since $K \subset J$, J/K is an ideal for $\mathcal{F}/K$.
   Question: What are ideals of $\mathcal{F}/J$? Since $\mathcal{F}/J \cong \mathbb{R}$ is a field then the ideals of $\mathcal{F}/J$ are $\mathcal{F}/J$ and $\{0_{\mathcal{F}/J}\}$.

Isomorphism Theorem

Theorem 1. Let $\varphi : R \to S$ to be the homomorphism of unitary rings. Let I to be the ideal of R and $I \subset \ker\varphi$. Then there exists a unique homomorphism of unitary rings $\overline{\varphi} : R/I \to S$ such that the following diagram commutes.



Namely $\overline{\varphi} \circ \pi = \varphi$, so $\overline{\varphi}(x + I) = \overline{\varphi}(\pi(x)) = \varphi(x)$.

Remark 3. Following the previous theorem, we have

1. $\text{Im}\,\overline{\varphi} = \text{Im}\,\varphi$, so $\overline{\varphi}$ is surjective if and only if φ is surjective.
2. $\ker\overline{\varphi} = \ker\varphi/I = \pi(\ker\varphi)$. So $\overline{\varphi}$ is injective if and only if $I = \ker\varphi$.

And we have a **corollary**: Let $\varphi : R \to S$ to be homomorphism of unitary rings. Still call $\Psi : R \to \varphi(R)$ with $x \mapsto \varphi(x)$ which is surjective. Take $I = \ker\varphi$ in the theorem and then $I = \ker\varphi = \ker\Psi$. Then $\overline{\Psi}$ is injective and surjective. Then $\overline{\Psi} : R/\ker\varphi \xrightarrow{\sim} \varphi(R)$, i.e. $R/\ker\varphi \cong \varphi(R)$.

Note: $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ then $\overline{\varphi} : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Lecture 5

Jan 21

Topic: Isomorphism Theorem; Vector space

Motivation of Isomorphism Theorem

Example 14. (Motivation of using isomorphism theorem) We know $f : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ by $x \mod 3 \mapsto x \mod 6$ is not well-defined since $0 \mod 3 = 3 \mod 3 \neq 3 \mod 6$. However, $g : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ by $x \mod 6 \mapsto x \mod 3$ is well defined homomorphism of unitary rings.

We want to have a more efficient proof of that fact. We want to apply isomorphism theorem to show g is well-defined homomorphism of unitary rings.

Introduce $\varphi : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ by $x \mapsto x \mod 3$ which is a well-known homomorphism of unitary rings. Since $\ker\varphi = 3\mathbb{Z} \supset 6\mathbb{Z}$. So there exists unique $\overline{\varphi} : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ such that $\varphi = \overline{\varphi} \circ \pi$ and $\overline{\varphi}(x + 6\mathbb{Z}) = \varphi(x)$ for any $x \in \mathbb{Z}$, namely $\overline{\varphi}([x]_6) = \varphi(x) = [x]_3$. So $g = \overline{\varphi}$.

Proof of Isomorphism Theorem and Corollaries

Proof. (Isomorphism Theorem) We introduce $\bar{\varphi} : R/I \to S$ by $r + I \mapsto \varphi(r)$. Then we would check:

1. $\overline{\varphi}$ is well defined. If $r + I = r' + I$, then $r - r' \in I \subset \ker\varphi$. So $\varphi(r' - r) = 0$ then $\varphi(r') = \varphi(r)$.
2. $\overline{\varphi}$ is an homomorphism of unitary rings. Note $\overline{\varphi} \circ \pi = \varphi$ implies the required unitary ring homomorphism $\overline{\varphi}$ has to be unique. $R/I = \{r + I | r \in R\} = \{\pi(r), r \in R\}$. Then $\overline{\varphi} : R/I \to S$ by $\varphi(r)$ since $\overline{\varphi}(\pi(r)) = \overline{\varphi} \circ \pi(r)$ forces $\overline{\varphi}(\pi(r))$ has to be $\varphi(r)$.
3. $\operatorname{Im}\varphi = \operatorname{Im}\varphi$ is true. $\overline{\varphi} \circ \pi = \varphi$ then $\operatorname{Im}\varphi \subset \operatorname{Im}\overline{\varphi}$. But π is surjective so we also have $\operatorname{Im}\overline{\varphi} \subset \operatorname{Im}\varphi$.
4. $\ker\overline{\varphi} = \ker\varphi/I$ is true. $\ker\overline{\varphi} = \{r + I | r \in R, \overline{\varphi}(r + I) = 0\} = \{\pi(r) | r \in R\varphi(r) = 0\} = \{\pi(r) | r \in R, r \in \ker\varphi\} = \pi(\ker\varphi) = \ker\varphi/I$.

Remark 4. We have a **corollary**.

1. R is a ring, I, J are two-sided ideals in R such that $I \subset J \subset R$.[We have shown J/I is an two- sided ideal of R/I], then $R/I\big/J/I \cong R/J$.

   Proof. We have $\varphi : R \xrightarrow{\pi_1} R/I \xrightarrow{\pi_2} R/I\big/J/I$ is a surjective homomorphism of rings. $\ker\varphi = \{r \in R | \pi_2(\pi_1(r)) = 0\} = \{r \in R | \pi_1(r) \in J/I\} = \{r \in R | \exists j \in J, \pi_1(r) = \pi_1(j)\} = \{r \in R | \exists j \in J, r - j \in \ker\pi_1 = I\} = \{r \in R | r \in J + I\} = J$ because $I \subset J$. By the first corollary of isomorphism theorem, $R/I\big/J/I \cong R/J$.

Remark 5. R is commutative ring and I is a two-sided ideal. R/I is a field if and only if I is a maximal ideal.

Proof. ($\Longrightarrow$) The ideal of a field k are $\{0\}$ and k. ($\Longleftarrow$) Let A be a commutative ring with only ideals A ($J = R$) and $\{0\}$ ($J = I$). We want to show A is a field. Let $a \in A \backslash \{0\}$. $\{0\} \neq Aa$ since $a \in Aa$ and $\{0\}$ is an ideal of A. So $Aa = A$ and $! \in Aa$. So there exists $b \in A$ such that $1 = ba = ab$.

Note. We have shown: k is a field $\Longleftrightarrow$ the ideals of k are $\{0\}$ and k.

Vector Space

Remark 6. $(V, +)$ is an abelian group. Then we define $\text{End}(V) := \{f : V \xrightarrow{\text{group}} V\}$ the set of group homomorphism. This is a ring for $\circ$ and $+$ with identity id_V. We can check $f \circ (g + h)(V) = f(g(V)) + f(h(V))$. In general, for group $(V, +)$ and $(W, +)$, $\text{Hom}_{\text{group}}(V, W) = \{f : V \xrightarrow{\text{group}} W\}$ is the set of group homorphism. Then if $V = W$, $\text{Hom}_{\text{group}}(V, V) = \text{End}_{\text{group}}(V)$.

Definition 13. (Vector Space, MATH 223) A triple $(V, +, \dot{})$ where V is a set and $+ : V \times V \longrightarrow V$ and $\cdot : k \times V \longrightarrow V$ which is $(\lambda, x) \mapsto \lambda x$ are maps is called vector space if

1. $\forall x, y, z \in V, (x + y) + z = x + (y + z)$
2. $\forall x, y \in V, x + y = y + x$.
3. $\exists 0 \in V$ such that $x + 0 = x$ for $\forall x$.
4. $\forall x \in V, \exists \tilde{x}$ such that $x + = 0$. (Notation: $\tilde{x} = -x$ and $x + (-y) = x - y$)
5. $\forall \lambda, \mu \in k, x \in V, \lambda(\mu x) = (\lambda\mu)x$.
6. $\forall x \in V, 1x = x$.
7. $\forall \lambda \in k, x, y \in V, \lambda(x + y) = \lambda x + \lambda y$.
8. $\forall \lambda, \mu \in k, x \in V, (\lambda + \mu)x = \lambda x + \mu x$

Definition 14. (Vector Space, Alternative Version) Let k to be a field, $(V, +)$ be a ablelian group. V is called a k-vector space if there exists an operation $k \times V \to V$ by $(\lambda, v) \to \lambda \cdot v$ such that $\Phi : k \to \text{End}_{\text{group}}(V)$ by $\lambda \mapsto \begin{pmatrix} V \to V \\ v \mapsto \lambda \cdot v \end{pmatrix}$ is a homomorphism of unitary rings.

We can check the equivalence.

1. $k \mapsto id_V$, then $1_k \cdot v = v$.
2. $\Phi(\lambda + \mu) = \Phi(\lambda) + \Phi(\mu)$, then for any $v \in V$, $(\lambda + \mu) \cdot v = \lambda v + \mu v$.
3. $\Phi(\lambda\mu) = \Phi(\lambda) \circ \Phi(\mu)$, for any $\lambda(\mu v) = (\lambda\mu)v$.
4. $\Phi(\lambda)$ is an endomorphism of groups. $\lambda(x + y) = \lambda x + \lambda y$.

Example 15. (Examples on Vector Space)

1. $k^n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, x_i \in k \right\}$ and $\lambda \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda \cdot x_1 \\ \vdots \\ \lambda \cdot x_n \end{pmatrix}$. For example $k = \mathbb{R}$.

2. $k[X] = \left\{ \sum_{i=0}^{\infty} a_i X^i \,\middle|\, n \in \mathbb{N}, a_i \in k \right\}$ is a k-vector space of polynomial in the variable X.

   We can write $P = \sum_{i=0}^{n} a_i X^i$ as $\begin{pmatrix} a_1 \\ \vdots \\ a_n \\ \vdots \end{pmatrix}$. And $\lambda \in k$, $P \in k[x]$, we have $\lambda \cdot P = \sum (\lambda a_i) X^i$.

3. $\mathcal{F} = \{f : \mathbb{R} \to \mathbb{R}\}$, $\lambda \in \mathbb{R}$. Then $\lambda \cdot f : \mathbb{R} \to \mathbb{R}$ by $x \mapsto \lambda(f(x))$.

Subvector Space

Definition 15. Let V be a k-vector space. $W \subset V$ is a sub-k-vector space of V if

1. $W \neq \emptyset$.
2. For any $\lambda_1, \lambda_2 \in k$, any $w_1, w_2 \in W$, $\lambda_1 w_1 + \lambda_2 w_2 \in W$.

Remark, The axiom implies $\vec{0} \in W$.

Example 16. (Examples on Subspace)

1. Solution of $\begin{cases} 2x + y = 0 \\ x + y = 0 \end{cases}$ is a subspace of $\mathbb{R}^2$.

2. If $P \in k[X]$ with coefficients not being all zero, we define $\deg(P) = \max\{i \leq N | a_i \neq 0\}$. If zero polynomial $P = \widetilde{0}$ with all coefficients 0, the $\deg \tilde{0} = -\infty$. Then the set $\{P \in k[X] | \deg(P) \leq s\}$ is a sub-k-vector space of $k[X]$.

3. Let V be a k-vector space and $X \subset V$, $X \neq \emptyset$. Then we define

$$\langle X \rangle := \left\{ \sum_{i=1}^{n} \lambda_i x_i, n \geq 1; x_i \in X; \lambda_i \in k \right\}$$

   This is a subspace called space generated by X.

Quotient Space

Definition 16. Let $W \subset V$ as a sub-k-vector space. Define V/W as a group. Let $k \times V/W \to V/W$ by $(\lambda, v + W) \mapsto \lambda v + W$. This map is well-define and provides a homomorphism of rings. $k \to \mathrm{End}_{group}(V/W)$. So V/W is a k-vector space.

Example 17. (Example of Quotient Space) $\mathcal{F}$ is a $\mathbb{R}$-vector space. $I = \{f \in \mathcal{F} | f(1) = 0\}$ is a subvector space. Then $\mathcal{F}/I$ is also a $\mathbb{R}$ vector space. We have shown in $\mathcal{F}/I$, $[f] = [\widetilde{f}(1)] = f(1)[\tilde{1}]$.

Lecture 6 Jan 23

Topic: Homomorphism of Vector Space; Generating Family and Basis; Finite Dimensions; k-algebra

Homomorphism of Vector Space

Definition 17. Let V, W be k-vector space, f is an homomorphism of k-vector space, also called k-linear transform, if $f(\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1 f(v_1) + \lambda_2 f(v_2)$ for any $\lambda_1, \lambda_2 \in k$, $v_1, v_2 \in V$. Then set of such homomorphism is denoted by $\mathrm{Hom}_k(V, W)$. Similarly, we have the set of endomorphism $\mathrm{End}_k(V) := \mathrm{Hom}_k(V, V)$.

Example 18. (Examples on Linear Transform)

1. $f : \mathbb{R}^2 \to \mathbb{R}^2$ by $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + 2y \\ 3x + 4y \end{pmatrix}$

2. $f : k[X] \to k[X]$ by $P \mapsto P'$ where if $P = \sum_{n \geq 0} a_n X^n$, $P' := \sum_{n \geq 1} a_n X^{n-1}$. f is a k-linear map by checking $f(\lambda P + \mu Q) = f\left(\sum_{n \geq 0} (\lambda a_n + \mu b_n) X^n\right) = \sum_{n \geq 1} (\lambda a_n + \mu b_n) n X^{n-1} = \lambda \sum_{n \geq 1} a_n X^{n-1} + \mu \sum_{n \geq 1} b_n X^{n-1} = \lambda f(P) + \mu f(Q)$. Actually, we can represent f as a matrix
$$[f]_{\{1, x, x^2, \ldots\}} = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots \\ 0 & 0 & 2 & 0 & \cdots \\ 0 & 0 & 0 & 3 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

3. Let $\mathcal{G} = \{f : \mathbb{R} \to \mathbb{R}, \text{differentiable}\}$, then $\varphi : \mathcal{G} \to \mathcal{F}$ by $f \mapsto f'$ is a linear map.

Generating Family of Vectors

Definition 18. (Basis)

1. V is a k-vector space. A collection/family of vector $(v_\alpha)_{\alpha \in A}$ is called k-linear independent if for any $n \in \mathbb{N}$, $\alpha_1, \ldots, \alpha_n \in A$, $\lambda_1, \ldots, \lambda_n \in k$, ${}_{i=1}^{n} \lambda_i v_{\alpha_i} = 0$ implies $\lambda_i = 0$ for all $i = 1, \ldots, n$.

2. A family of vector $(v_\alpha)_{\alpha \in A}$ is a generating family for V if any $v \in V$, there exists $n \in \mathbb{N}$, $\lambda_1, \ldots, \lambda_n \in k$ such that $v = \sum_{i=1}^{n} \lambda_i v_{\alpha_i}$ where $\alpha_1, \ldots, \alpha_n \in A$.

3. A collection of vector space is called a basis if it is a linearly independent and is a generating family.

Finite Dimension

Proposition 4. Let V be a k-vector space and suppose that $\{v_1, \dots, v_n\}$ is a (finite) generating family. One can extract from that family a basis for V.

Lemma 1. If V has a basis with n vectors, then any linearly independent family in V has cardinality less then or equal to n.

Remark 7. If V has a basis with cardinality n, then any other basis has cardinality n.

Definition 19. If V has a basis with cardinality, we same the dimension, $\dim V = n$.

Proposition 5. If V has $\dim V = n$, then

1. A linearly independent family of n vectors is a basis.
2. A generating family of n vector is a basis.

Example 19. (Examples on Dimension)

1. $V = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3 \middle| \begin{cases} x+y+z=0 \\ x+3y+4z=0 \end{cases} \right\}$ then $\dim V = 1$.

2. k^n has dimension n and the canonical basis is $\{e_1, \dots, e_n\}$ where $e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$ where 1 is on the i-th row.

3. $k[X]$ has infinite dimension while $\{P \in k[X] | \deg P \leq n\}$ is a sub-vector space with dimension $n+1$ and basis $\{1, x, x^2, \dots, x^n\}$.

4. $M_n(k)$ has dimension n^2 over k so as vector space $M_n(k) \cong k^{n^2}$.
   Define the unique linear transformation $f : k^n \to V$ by $e_i \mapsto v_i$ where e_i is i-th vector is isomorphic. Also $\text{End}_k(V)$ is a k-vector space. Then the map $\text{End}k(V) \to M_n(k)$ by $f \mapsto [f]_{v_1,\dots,v_n}$ is an isomorphism of vector spaces. So as vector spaces $\text{End}_k(V) \cong M_n(k) \cong k^{n^2}$.

Proposition 6. (Dimension of Quotient Spaces and of Linear Maps)

1. V is a n-dimensional vector space and $W \subset V$ is a subspace with $\dim W =\leq n$. Then $\dim V/W = n - m$.

2. V, W are finite dimensional vector spaces. For a linear map $f : V \to W$, we have $\dim V = \dim \ker f + \dim \operatorname{Im} f$.
   Corollary: If $f : V \to V$, then f is injective if and only if f is surjective.

k-algebra

Example 20. (A motivation Example) $k[X] = \left\{ \sum_{n \geq 0} a_n X^n, a_n \in k, \text{finitely many } a_n \neq 0 \right\}$.
For $P = \sum_{n \geq 0} a_n X^n$ and $Q = \sum_{n \geq 0} b_n X^n$, we can define $P \times Q = \sum_{\ell \geq 0} c_\ell X^\ell$ where $c_\ell := \sum_{n=0}^{\ell} a_n b_{\ell - n}$. One can check that $P \times (\lambda Q + \mu R) = \lambda(P \times Q) + \mu(P \times R)$ where $P, Q, R \in k[X]$ and $\lambda, \mu \in k$.
We have a summary. $k[X]$ is a k vector space then $(k[X], +)$ is a group. We define a product on $k[X]$ and one can check that $(k[X], +, \times)$ is a unitary and commutative ring (with $\tilde{0}, \tilde{1}$). And the product $\times$ behaves well with respect to the structure of vector space, we say that $k[X]$ is a k-algebra.

Remark 8. We can put it more formally.

1. Let R be a ring and k is a field. Suppose we have a homomorphism of unitary rings, $k \to R$. since the kernel as an ideal of a field can only be k or $\{0\}$. $\ker = k$. Then the homomorphism is injective.

2. Let R be a unitary ring and suppose that it contain the field of k as subring. For example, we consider k as a subring of $k[X]$ while in fact $k[X]$ only contains a copy of k with the injective homomorphism, $k \hookrightarrow k[X]$ by $\lambda \to \widetilde{\lambda}$.

3. In more general, if k is contained in the center of R, then R is called a k-algebra.
   Note. R is then naturally a k-vector space via $k \times R \to R$ by $(\lambda, r) \mapsto \lambda \times r$. One can check that $\lambda \cdot (r_1 \times r_2) = r_1 \times (\lambda \cdot r_2)$ and $r_1 \times (\lambda_2 r_2 + \lambda_3 r_3) = \lambda_2(r_1 \times r_2) + \lambda_3(r_1 \times r_3)$ since λ commutes with everyone.

Lecture 7 Jan 28

Topic: k-algebra; Group Rings; Polynomial Rings

k-algebra

Definition 20. Let $(A, +, \times)$ be a unitary ring. We say that A is k-algebra if A contain k in its center. *Equivalently*, we say A is a k-algebra if it is equipped with a structure of k-vector space $k \times A \to A$ by $(\lambda, a) \mapsto \lambda \cdot a$ such that $\lambda \cdot (a \times b) = (\lambda \cdot a) \times b = a \times (\lambda \cdot b)$ for any $\lambda \in k$ and $a, b \in A$.

Definition 21. Let $(A, +, \times, \cdot)$ be a k-algebra. Let $(B, +, \times)$ be a subring of A with the same unit. Then B is a sub-k-algebra of A if it is also a sub-k-vector space. Namely for any $\lambda_1, \lambda_2 \in k$ and any $b_1, b_2 \in B$, we have $\lambda_1 \cdot b_1 + \lambda_2 \cdot b_2 \in B$.

Definition 22. Let $(A, +, \times, \cdot)$ and $(B, +, \times, \cdot)$ be two k-algebra. A homomorphism of unitary rings $f : A \to B$ is a homomorphism of k-algebra if f is also k-linear ($f(\lambda \cdot 1_A) = \lambda \cdot 1_B$).

Example 21. (Examples on k-algebra and k-algebra homomorphism)

1. $k[x]$ is a k-algebra. Let $f : k[X] \to k[X]$ be the unique homomorphism of k-algebra such that $X \mapsto X^2$. It is image is a sub-k-algebra of $k[X]$. It is the smallest sub-k-algebra containing X^2. It is denoted by $k[X^2]$.

2. Let $(G, \circ)$ be a group. List of its elements $G = g|g \in G$. $k[G]$ is a k-vector space with basis $\{e_g\}_{g\in G}$. $k[G]$ has a natural structure of k-algebra where the multiplication $\times$ is given by $e_g \times e_{g'} := e_{g\circ g'}$. Then $(\lambda_1 e_{g_1} + \lambda_2 e_{g_2}) \times (\lambda_3 e_{g_3} + \lambda_4 e_{g_4}) = \lambda_1\lambda_3 e_{g_1\circ g_3} + \lambda_1\lambda_4 e_{g_1\circ g_4} + \lambda_3\lambda_3 e_{g_2\circ g_3} + \lambda_2\lambda_1 e_{g_2\circ g_4}$. We have the following quick facts:

   - If G is finite, $|G| = n$, then $k[G]$ has dimension n as a k-vector space.
   - If $(G, \circ)$ is abelian, then $k[G]$ is a commutative ring/algebra.
   - If $H < G$ is a subgroup of G, then $k[H]$ is a subalgebra of $k[G]$.
   - The unique homomorphism of k-vector space such that $f : k[G] \to k$ by $e_g \mapsto 1_k$ for all $g \in G$ is in fact a homomorphism of k-algebra because $f(e_g \times e_{g'}) = f(e_{g\circ g'}) = 1_k$. Then the kernel $\ker f$ is subspace with basis $\{e_g - e_{1_G}\}_{g\in G\setminus\{1_G\}}$.
     Proof. $e_g - e_{1_G} \in \ker f$ then the subspace generated by $\{e_g - e_{1_G}\}_{g\in G\setminus\{1_G\}}$ is a subset of $\ker f$. Let $x = \sum \lambda_g e_g \in \ker f$. Then means $\sum \lambda_g = 0$. So $x = \sum \lambda_g e_g - (\sum \lambda_g) e_{1_G} = \sum \lambda_g (e_g - e_{1_G})$.

Polynomial over a Ring

Definition 23. Let R be a unitary ring. Suppose it's commutative. Define $R[X] = \left\{\sum_{i=0}^{n} r_i X^i, n \in \mathbb{N}, r_i \in R\right\}$.

Claim: $R[X]$ is a unitary ring with identity $\tilde{1} = 1X^0$. Then we could check the addition and multiplication.

$$\sum_{i=0}^{n} r_i X^i + \sum_{i=0}^{m} s_j X^j = \sum_{\ell=0}^{\max(m,n)} (r_\ell + s_\ell) X^\ell$$

where we set $s_\ell = 0$ if $\ell \geq m+1$ and $r_\ell = 0$ if $\ell \geq n+1$. And

$$\sum_{i=0}^{n} r_i X^i \times \sum_{i=0}^{m} s_j X^j = \sum_{\ell \geq 0} t_\ell X^\ell$$

where $t_\ell = \sum_{i=0}^{\ell} r_i s_{\ell-i}$.

Example 22. $\mathbb{Z}[X]$ is a subring of $\mathbb{Q}[X]$.

Definition 24. Degree of $P = \sum_{i=0}^{n} r_i X^i \in R[X]$ is defined as

$$\deg P = \begin{cases} \max\{i : a_i \neq 0\} & \text{if} P \neq \\ -\infty & \text{if} P = \tilde{0} \end{cases}$$

We say the dominate of $P = \sum_{i=0}^{n} r_i X^i$ with degree $d \geq 0$ is r_d. P is said to be monic if $r_d = 1_R$. [e.g. $X^2 + 3X - 2$ is monic in $\mathbb{Z}[X]$].

Lemma 2. Let $A, B \in R[X]$, then

1. $\deg(A+B) \leq \max\{\deg A, \deg B\}$
2. $\deg(AB) = \deg A + \deg B$ if R is an integral domain.

Example 23. Let $R = \mathbb{Z}/4\mathbb{Z}$, then $(\overline{2}X + \overline{2})(\overline{2}X^3) = \overline{4}X^4 + \overline{2}X^3 = \overline{2}X^3$. We see $\deg(AB) = 3 \neq 1 + 3 = \deg A + \deg B$.

Lemma 3. If R is an integral domain, $(R[X])^\times = R^\times = \{r \cdot \tilde{1} | r \in R^\times\}$.

Proof. (1) $P = r \cdot \tilde{1} = \tilde{r} = rX^0$ with $R \in R^\times$ then $Q = \widetilde{r^{-1}}$. Thus $PQ = \tilde{1}$. Then $R^\times \subset (R[X])^\times$. (2) If $P \in (R[X])^\times$, let Q be its inverse. $PQ = \tilde{1}$. Then $\deg P + \deg Q = 0$. Then $\deg P = \deg Q = 0$. So P, Q are constant polynomial. $P = \widetilde{r}$ and $Q = \widetilde{s}$. $PQ = \tilde{1}$. Then $rs = 1$. So $r \in R^\times$.

Example 24. $(\mathbb{Z}/4\mathbb{Z}[X])^\times = \{2P + 1 | P \in \mathbb{Z}/4\mathbb{Z}[X]\}$. $(2P+1)^{-1} = -2P + 1$.

Definition 25. Let R be an integral domain. $P \in R[X]\backslash\{0\}$ is irreducible if $P = AB$ with $A, B \in R[X]$ implies $A \in R^\times$ or $B \in R^\times$.
Note. The basic idea is to decompose P into two polynomials A, B but it would not be interesting to have $A \in R^\times$ since any $P \in R[X]$ can be written as $P = 1P = A^{-1}AP = A^{-1}P'$.

Proposition 7. If R is an integral domain, then $R[X]$ is also an integral domain.
Proof. Let $A, B \in R[X]$. Suppose $AB = 0$ then $\deg A + \deg B = \infty$. So $\deg A = -\infty$ or $\deg B = -\infty$. So $A = 0$ or $B = 0$.

Remark 9. If R is an integral domain, $R[X]$ has an fraction field. [e.g frac($\mathbb{Z}[X]$) = $\mathbb{Q}(X)$??]

Example 25. Let R be a unitary commutative ring. $S := R[X]$ is a unitary commutative ring. Build $S[Y] = R[X][Y] = \left\{\sum_{i\geq 0}\left(\sum_{j\geq 0} r_{ij}X^j\right)y^i\right\} = \left\{\sum_{i\geq 0}\sum_{j\geq 0} r_{ij}X^jY^i\right\}$. We usually denote $R[Y][X]$ by $R[X, Y]$. We would show later that $\mathbb{R}[X, Y]/(Y - X^2) \cong \mathbb{R}[T]$.

Polynomial over a Field $R = k$

Theorem 2. (Euclidean Division in $k[X]$) Let $A, B \in k[X]$. Suppose $B \neq \widetilde{0}$, there exists unique $(Q, R) \in k[X]^2$ such that $A = BQ + R$ where $\deg R < \deg B$. [e.g. $X^3 + X + 1 = (X + 1)(X^2 - X + 2) - 1$]

Definition 26. We say B divides A, $B|A$ if $R = 0$ in the Euclidean division.

Example 26. If $B = X - \lambda$ for $\lambda \in k$, what is the remainder R in the division $A = BQ + R$? We know $R = \tilde{r}$ by degree comparison. Then by $A = (x - \lambda)Q + \tilde{r}$, $A(\lambda) = r$ (evaluated at λ). Therefore $R = \widetilde{A(\lambda)}$.

Remark 10. If R is a unitary ring, $\lambda \in R$. We define $f_\lambda : R[X] \to R$ by $P = \sum r_i X^i \mapsto \sum r_i \lambda^i$. This is a homomorphism of rings called evaluation at λ. We write $P(\lambda) = \sum r_i \lambda^i$.

Lecture 8

Jan 30

Topic: Polynomial Ring over a field: Euclidean Division, Principle Ideals, Induced Homomorphism, Evaluation Map.

Euclidean Division

In general, let $A, B \in k[X]$. Suppose $B \neq \widetilde{0}$, there exists unique $(Q, R) \in k[X]^2$ such that $A = BQ + R$ where $\deg R < \deg B$.

Example 27. Continued from the previous example. We have shown that if $B = X - \lambda$ where $\lambda \in k$. Then $A = QB + \widetilde{A(\lambda)}$. Therefore $X - \lambda | A$ if and only if $A(\lambda) = 0$. In that case we say λ is a root of A. Given a root $\lambda \in k$ for $A \in k[X]$, we call multiplicity of λ as the number $\max\{m \in \mathbb{N} | (X - \lambda)^m | A\}$.

Proposition 8. If A has degree n, it has at most n roots counted with multiplicity.
Proof. By induction on $\deg A$. Base case: $A = \lambda_1 X + \lambda_2$ with one root. Inductive step, $A = (X - \lambda)^m C$ then $\deg C = n - m$.

Ideals of $k[X]$

Proposition 9. The ideal of $k[X]$ are all of the form $pk[X] = (P)$ where P can be picked to be monic.
Proof. Let I be an ideal of $k[X]$. (1) If $I = \{0\}$, then $I = (0)$. (2) Otherwise $I \neq \{0\}$ so it contains a non-zero polynomial. Let $u_0 = \min\{u \geq | \exists P \in I, \deg P = n\}$. Let $P_0 \in I$ with degree n_0. One can choose P_0 to be monic. If P_0 is not monic, we can find $\lambda \in k$ such that $\lambda^{-1} P \in I$ is monic. Then $(P_0) \subset I$ since $P_0 \in I$. We want show $I \subset (P_0)$. Let $A \in I$ and we apply Euclidean division on A by P_0, $A = P_0 Q + R$, $\deg R < \deg P_0$. Then $R = \underbrace{A}_{\in I} - \underbrace{P_0 Q}_{\in I} \in I$. However $\deg R < \deg P = n_0$. Then $R = 0$ so $A \in (P_0)$.

Corollary: Let $P \in k[X] \backslash \{0\}$. Then the following three statements are equivalent:

1. P is irreducible.
2. $k[X]/(P)$ is an integral domain.
3. $k[X]/(P)$ is a field.

Proof. ($3 \implies 2 \implies 1$) Assume $k[X]/(P)$ is a field. Then $k[X]/(P)$ is an integral domain. Let $A, B \in k[X]$ such that $P = AB$. It implies that $\overline{AB} = \overline{0}$ in $k[X]/(P)$. So $\overline{A} = \overline{0}$ or $\overline{B} = \overline{0}$, namely $P|A$ or $P|B$. For example $P|A$ so $\deg P \leq \deg A$. But also $A|P$ so $\deg A \leq \deg P$ so $\deg A = \deg P$. But $P = AB$ so $\deg B = 0$. So $B \in k^\times$. We proved that if $P = AB$ then $A \in k^\times$ or $B \in k^\times$. So P is irreducible.

$(1 \implies 3)$ Assume P is irreducible. We want to show that $k[X]/(P)$ is a field. Let J be an ideal of $k[X]$ such that $(P) \subset J \subset k[X]$. There exists $P_0 \in k[X]$ such that $J = (P_0)$ so $(P) \subset (P_0)$. Then $P \in (P_0)$ and we can find $A \in k[X]$ such that $P = P_0 A$. Then $P_0 | P$. But P is irreducible so either $P_0 \in k[X]$ or $A \in k^\times$. Then either $J = (P_0) = k[X]$ or $J = (P_0) = (P)$. Then (P) is maximal and $k[X]/(P)$ is a field.

Remark 11. $2x$ is irreducible in $\mathbb{Q}[X]$ or $\mathbb{R}[X]$ but not irreducible in $\mathbb{Z}[X]$. $P = 2x = 2 \cdot x$ where $2, X \notin \mathbb{Z}^\times$.

Induced Maps

Consider homomorphism of unitary rings $f : R \to S$. We define $\widetilde{f} : R[X] \to S[X]$ by $\sum r_i X^i \mapsto f(r_i) X^i$.

Example 28. Examples on Induced Maps

1. R is an integral domain and S is a field of fraction of R. [e.g. $R = \mathbb{Z}$, $S = \mathbb{Q}$]. Let $f : R \hookrightarrow S$ by $r \mapsto \frac{r}{1}$ then $\widetilde{f} : R[X] \hookrightarrow S[X]$ is an injection. So we identify $R[X]$ as a subring of $S[X]$.
2. $R = \mathbb{Z}$ and $S = \mathbb{Z}/n\mathbb{Z}$. $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Then $\widetilde{\pi} : \mathbb{Z}[X] \to \mathbb{Z}/n\mathbb{Z}[X]$ is surjective and $\ker \widetilde{\pi} = n\mathbb{Z}[X]$ as the ideal of $\mathbb{Z}[X]$ generated by n. Then by isomorphism theorem, $\mathbb{Z}/n\mathbb{Z}[X] \cong \mathbb{Z}[X]/n\mathbb{Z}[X]$ as rings.
3. In more general, let be an ideal of the ring R and let $I[X]$ denote the ideal of $R[X]$ generated by I, then $R[X]/I[X] \cong (R/I)[X]$.

Evaluation Maps

Let R to be a commutative ring, $r_0 \in R$. Then $ev_{r_0} : R[X] \to R$ by $\sum a_i X^i \mapsto \sum a_i \lambda_0^i$ is the unique homomorphism of rings $R[X] \to R$ that fixes R and sends X to r_0. ev_{r_0} is always subjection so $R \cong R[X]/\ker ev_{r_0}$ as rings. Then what is the kernel?

Example 29. Kernel of Evaluation Maps.

1. $R = k$ is a field and r_0 is noted as λ. $ev_\lambda : k[X] \to k$. Since $X \mapsto \lambda$, we know $X - \lambda \mapsto 0$. Then we want to show $(X - \lambda) = \ker ev_\lambda$. (1) We know $(X - \lambda) \subset \ker ev_\lambda$ since $X - \lambda \in \ker ev_\lambda$. (2) Let $P \in \ker ev_\lambda$, $ev_\lambda(P) = P(\lambda) = 0$. Then by Euclidean division $P = (X - \lambda)Q + P(\lambda) = (X - \lambda)Q$. So $P \in (X - \lambda)$. So $\ker ev_\lambda \subset (X - \lambda)$. Therefore, $k[X]/(X - \lambda) \cong k$ as rings, k-algebra and k-vector space. Note $\dim k[X]/(X - \lambda) = 1$ with basis $\tilde{1}$.
2. $R = \mathbb{Z}/4\mathbb{Z}$ and $r_0 = \overline{2}$. Then $ev_{\overline{2}} : \mathbb{Z}/4\mathbb{Z}[X] \to \mathbb{Z}/4\mathbb{Z}$ by $X \mapsto \overline{2}$. We know $X - \overline{2} \in \ker ev_{\overline{2}}$ and then $(X - \overline{2}) \subset \ker ev_{\overline{2}}$. However we can't do Euclidean division here. Note $X^2, \overline{2}X \in \ker ev_{\overline{2}}$ but $X^2 = (X - \overline{2})(X + \overline{2})$ and $\overline{2}X = \overline{2}(X - \overline{2})$.
3. $R = \mathbb{Z}$ and $r_0 = 2$. We have $ev_2 : \mathbb{Z}[X] \to \mathbb{Z}$ by $X \mapsto 2$. We know $(X - 2) \subset \ker ev_2$. But we can also show $\ker ev_2 \subset (X - 2)$. Let $P \in \ker ev_2$, we can do Euclidean division of P by $X - 2$ in $\mathbb{Q}[X]$. We have $P = (X - 2)Q + P(2) = (X - 2)Q$. Since $X - 2$ is monic, $Q \in \mathbb{Z}[X]$.

Remark 12. A useful tool to "apply" Euclidean division on integral domain R. Let R be an integral domain. We know $R[X] \hookrightarrow \text{frac}(R)[X]$. Let $A.B \in R[X]$, $B \neq 0$. Let $k := \text{frac}(R)$. One can compute Euclidean division of A by B in k[X]. There exists unique $(Q,T) \in k[X]^2$ such that $A = BQ + T$. If $B \in R[X]$ is monic (or other coefficient in $R^\times$), then $(Q,T) \in R[X]$. It's not hard to see, because for the following example,

$$\begin{array}{r|l} & \frac{1}{2}X + \frac{1}{4} \\ \hline 2X+1 & X^2 + X + 1 \\ & -X^2 - \frac{1}{2}X \\ \hline & \frac{1}{2}X + 1 \\ & -\frac{1}{2}X - \frac{1}{4} \\ \hline & \frac{3}{4} \end{array}$$

we know it is always the leading term determine the coefficients in (Q,T).

Lecture 9

Feb 4

Topic: Revisit of Homomorphism of k-algebra; Revisit of Evaluation Map; Prime Ideals; Max Ideals.

Homorphism of k-algebra

Recall the definition: Let $(A, +, \times, \cdot)$ and $(B, +, \times, \cdot)$ be two k-algebra. A homomorphism of unitary rings $f : A \to B$ is a homomorphism of k-algebra if f is also k-linear. What is the k-linear here? We can define it in two equivalent ways.

- $f(\lambda_1 a_1 + \lambda_2 a_2) = \lambda_1 f(a_1) + \lambda_2 f(a_2)$. Then for any $\lambda \in k$ $f(\lambda \cdot 1_A) = \lambda \cdot 1_B$. In some sense $f(\lambda) = \lambda$, which identifies λ in B.
- $f(\lambda \cdot 1_A) = \lambda \cdot 1_B$. Thus $f(\lambda_1 a_1 + \lambda_2 a_2) = f((\lambda_1 \cdot 1_A) \times a_1 + (\lambda_2 \cdot 1_A) \times a_2) = f(\lambda_1 \cdot 1_A) \times f(a_1) + f(\lambda_2 \cdot 1_A) \times f(a_2) = \lambda_1 f(a_1) + \lambda_2 f(a_2)$.

Revisit of Evaluation Map

Recall $ev_x : k[X] \to k$ by $P = P(x)$, fix $x \in k$ and k is a field. We have shown that $\ker ev_x = (X - x)$. Then $k[X]/(X - x) \cong k$ as a ring.

By isomorphism theorem, we can introduce $\overline{ev}_\lambda : P \mod (X - x) \mapsto P(x)$. Notice that $\overline{ev}_x(\widetilde{\lambda} \mod (X - x)) = \widetilde{\lambda}(x) = \lambda$. So ev_x fixes k. So $\overline{ev}_x$ is an homomorphism of k-algebras. Therefore $k[X]/(X - x) \cong k$ as an k-algebra. So as a k-vector space.

$P \in k[X] \backslash \{0\}$ with $\deg P = n$. We can check that $k[X]/(P)$ is a k-algebra as a vector space with dimension n.

Example 30. What is the kernel of $\overline{ev}_r : \mathbb{Z}/6\mathbb{Z}[X] \to \mathbb{Z}/6\mathbb{Z}$?

Remark 13. Difference between polynomial functions $P : k \to k$ and polynomials. Consider the map

$$\begin{aligned} F : \quad & k[X] \to \text{Functions}(k \to k) \\ & P \mapsto (\lambda \mapsto ev_\lambda(P) =: P(\lambda)) \end{aligned}$$

The image of this map is the ring of polynomial functions $k \to k$. By definition, $k[X] \to$ polynomial functions $(k \to k)$ is surjective. For injectivity, we know $P \in \ker F$ if and only if for any $\lambda \in k$, $P(\lambda) = 0$. We say that if P has degree $n \geq 0$, then P has at most n roots. Then k is infinite, $\ker F = \{0\}$. If $k = \mathbb{Z}/p\mathbb{Z}$ with p prime. We can let $P := (X - 1)(X - 2) \cdots (X - p)$ has degree p and $P \in \ker F$. Then F is not injective.

Maximal Ideal

Definition 27. M is an left/right/two-sided ideal of R. M is called maximal ideal if

1. $M \neq R$.
2. For any J ideal of R such that $M \subset J \subset R$, $M = J$ or $J = R$.

Theorem 3. If R is a unitary ring, then every proper (left/right/two-sided) ideal of R is contained in a maximal ideal.
Proof. By Zorn's Lemma.
Corollary: R is a unitary ring then it contains at least one ideal.

Proposition 10. If R is a unitary commutative ring and I is a proper ideal of R, then I is maximal if and only if R/I is a field.

Example 31. Maximal ideals.

1. $\mathbb{C}[X]$. $P \neq 0$. We have shown that P is irreducible if and only if $k[X]/(P)$ is an integral domain, if and only if $k[X]/(P)$ is a field. Then the maximal ideals are $(X - \lambda)$ where $\lambda \in \mathbb{C}$.
   Note. I is a proper ideal of $\mathbb{C}[X]$. There exists $P \in \mathbb{C}[X]$ such that $I = (P)$. P has a root λ then $(X - \lambda)|P$ which implies $(P) \subset (X - \lambda)$.
2. $\mathbb{R}[X]$. Take the roots $\alpha_i \in \mathbb{C}$ of $P \in \mathbb{C}[X]$. Then we can write $P = \prod(X - \alpha_i) \in \mathbb{C}[X]$. We know $P(\overline{\alpha}_i) = \overline{P(\alpha_i)} = 0$. This shows α_i and $\overline{\alpha_i}$ are both roots of P. Then we can match them in pair if $\operatorname{Im} \alpha_i \neq 0$, $(X - \alpha_i)(X - \overline{\alpha}_i) = X^2 - 2(\mathrm{Re}\alpha_i)X + |\alpha_i|^2$. Or if α_i is purely real, it is just $X - \alpha_i$. Then the irreducible polynomials are in the form $X - a$ where $a \in \mathbb{R}$ or $X + aX + b$ where $a, b \in \mathbb{R}$ such that $a^2 - 4b < 0$. Then the maximal ideals are in the form $(X - a)$ where $a \in \mathbb{R}$ or $(X + aX + b)$ where $a, b \in \mathbb{R}$ such that $a^2 - 4b < 0$.

Prime Ideals

Definition 28. Let R be a ring and P is a proper ideal of R. We say P is a prime ideal if for any $x, y \in R$, $xy \in R$ implies $x \in R$ or $y \in R$.

Proposition 11. If R is a unitary commutative ring, I is a proper ideal of R. Then I is prime if and only if R/I is an integral domain.

Example 32. Prime ideals.

1. In $k[X]$, prime ideals $=$ maximal ideal $= \{(P) | P \text{ irreducible}\}$. [$R/I$ is field is equivalent to R/I is an integral domain in $k[X]$]
2. In $\mathbb{Z}$, prime ideals $=$ maximal ideal $= \{(P) | P \text{ prime}\}$.

Proposition 12. Let R be a unitary ring. Then I is a maximal ideal implies I is a prime ideal.

Example 33. Prime ideal but not maximal ideal. Let $R = \mathbb{Z}[X]$.

1. Consider the map $f : \mathbb{Z}[X] \to \mathbb{Z}$ by $P \mapsto P(0)$. Since the kernel $\ker f = (x)$, $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$. (X) is prime but not maximal.
2. With natural map $\pi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, we can compose $g = \pi \circ f : \mathbb{Z}[X] \to \mathbb{Z}/2\mathbb{Z}$ by $P \mapsto P(0) \mod 2$. Then $\ker g \supset \ker f = (X)$. And since $\mathbb{Z}[X]/\ker g \cong \mathbb{Z}/2\mathbb{Z}$, $\ker g$ is the maximal ideal. $P \in \ker g$ means $P(0) = 0 \mod 2$. Then P is in the form of $\sum a_i X^i + 2a_0$, $a_i \in \mathbb{Z}$. So $\ker g = (X) + (2) = X\mathbb{Z}[X] + 2\mathbb{Z}[X] = (X, 2)$.

Example 34. Maximal Ideals.

1. Maximal ideal of $\mathbb{C}[X, Y]$ are ideals of the form $(X - a, Y - b)$ where $a, b \in \mathbb{C}$.
2. A is finite dimensional $\mathbb{C}$-algebra. $\text{Spec}(A)$ would be the set of prime ideals of A on which there is neutral top.

Lecture 10

Feb 6

Topic: An example on Polynomial Rings; Chinese Remainder Theorem.

An example on Polynomial Rings

1. We want to show $\mathbb{R}[X,Y]/(Y-X^2) \cong \mathbb{R}[T]$ as $\mathbb{R}$-algebra. We want to find $f : \mathbb{R}[X,Y] \to \mathbb{R}[T]$ such that $(Y - X^2) \subset \ker f$. Such f is determined by the image $f(X)$ and $f(Y)$.

   We could try $f(Y) = T^2$ and $f(X) = T$. Then $f(\sum a_{ij}X^iY^j) = \sum a_{ij}T^iT^{2j}$. Then $f(Y - X^2) = T^2 - T^2 = 0$ and $(Y - X^2) \subset \ker f$. Then by isomorphism theorem, there exists $\overline{f} : \mathbb{R}[X,Y]/(Y - X^2) \to \mathbb{R}[T]$ by $P(X,Y) \mod (Y - X^2) \mapsto f(P) = P(T,T^2)$.

   We can find the inverse of $\overline{f}$. Let $g : \mathbb{R}[T] \to \mathbb{R}[X,Y]$ by $Q(T) \mapsto Q(X) \mod Y - X^2$. Then $g \circ \overline{f}(X \mod Y - X^2) = g(f(X))) = g(T) = X \mod Y - X^2$. And $g \circ \overline{f}(Y \mod Y - X^2) = g(f(Y)) = g(T^2) = X^2 \mod Y - X^2 = Y \mod Y - X^2$. Then $g \circ \overline{f} = Id$ and g is the inverse of $\overline{f}$.

2. What are the prime ideals of $\mathbb{R}[X,Y]/(Y - X^2)$? Since $\mathbb{R}[X,Y]/(Y - X^2) \cong \mathbb{R}[T]$, we can find the prime ideals in $\mathbb{R}[T]$ and map it back to $\mathbb{R}[X,Y]/(Y - X^2)$.

   As we have shown in the last lecture, to find the prime ideal $(Q) \subset \mathbb{R}[T]$ is to find the irreducible polynomial $Q \in \mathbb{R}[T]$. The irreducible polynomial in $\mathbb{R}[T]$ has the form $T - \alpha$, $\alpha \in \mathbb{R}$ or $T^2 + \alpha T + \beta$, $\alpha, \beta \in \mathbb{R}$ such that $\alpha^2 - 4\beta < 0$.

   Then the prime ideals of $\mathbb{R}[X,T]/(Y-X^2)$ is the image by g of $(T-\alpha)$ and $(T^2+\alpha T+\beta)$. We have
$$g((T-\alpha)) = (\overline{T-\alpha}) = (X-\alpha, Y - X^2)/(Y - X^2)$$
$$g((T^2+\alpha T+\beta)) = (\overline{X^2+\alpha X+\beta}) = (X^2+\alpha X+\beta, Y - X^2)/(Y - X^2)$$
   We can see there are two kinds of max/prime ideals in $\mathbb{R}[X,Y]/(Y - X^2) = A$ as a $\mathbb{R}$-algebra. We write
$$(X-\alpha, Y - X^2)/(Y - X^2) = (X-\alpha, Y-\alpha^2)/(Y - X^2) = I_\alpha$$
$$(X^2+\alpha X+\beta, Y - X^2)/(Y - X^2) = (X^2+\alpha X+\beta, Y+\alpha X+\beta) = I_{\beta,\gamma}$$
   [*Note.* $(X-\alpha, Y-X^2) = (X-\alpha, Y-\alpha^2)$ because (1) $Y - X^2 = Y - \alpha^2 + \alpha^2 - X^2 = Y - \alpha^2 - (X-\alpha)(X+\alpha) \in (X-\alpha, Y-\alpha^2)$ and (2) $Y - \alpha^2 = (Y-X^2) + (X-\alpha)(X+\alpha) \in (X-\alpha, Y-X^2)$] Then we have
$$A/I_\alpha \cong \mathbb{R}[T]/(T-\alpha) \cong \mathbb{R}, \dim A/I_\alpha = 1$$

$$A/I_{\beta,\gamma} \cong \mathbb{R}[T]/(T^2+\beta T+\gamma) \cong \mathbb{R}^2, \dim A/I_{\beta.\gamma} = 2$$

[*Note.* $A/I_\alpha = \mathbb{R}[X,Y]/(Y-X^2)\big/(X-\alpha, Y-X^2)/(Y-X^2) \cong \mathbb{R}[X,Y]/(X-\alpha, Y-X^2)$. Then $P \in \mathbb{R}[X,Y]$, $P \in R[X][Y]$. $P = (Y-X^2)Q + R$ where $Q \in \mathbb{R}[X,Y]$ and $R \in \mathbb{R}[X]$. Then $P = \underbrace{(Y-X^2)Q + (X-\alpha)S}_{T_\alpha} + R(\alpha) \equiv R(\alpha) \mod I_\alpha \equiv R(\alpha)(1 \mod I_\alpha)$]

[*Note.* $A \cong \mathbb{R}$ and $\overline{f}((\overline{X-\alpha})) = (X-\alpha)$. Therefore $A/I_\alpha \cong \mathbb{R}[T]/(T-\alpha)$.]

3. Spectrum of A. As a set, $\mathrm{Spec}(A) = \{\alpha, \alpha \in \mathbb{R}, (\beta.\gamma), \beta, \gamma \in \mathbb{R}, \beta^2 - 4\gamma < 0\}$. Consider the homomorphism of $\mathbb{R}$-algebra $\varphi : A \to \mathbb{R}$. Kernel of φ is an ideal of A such that $A/\ker\varphi \cong \mathbb{R}$. There exists $\alpha \in \mathbb{R}$ such that $\ker\varphi = I_\alpha = (X-\alpha, Y-\alpha^2)/(Y-X^2)$. Then $\varphi(X \mod Y-X^2) = \varphi(X-\alpha \mod Y-X^2+\alpha \mod Y-X^2) = \varphi(\alpha \mod Y-X^2) = \alpha\varphi(1 \mod Y-X^2) = \alpha$. And $\varphi(Y \mod Y-X^2) = \varphi(\alpha^2 \mod Y-X^2) = \alpha^2$. Then there is a one to one correspondence between I_α and points on the curve $y = x^2$.

Chinese Remainder Theorem

Definition 29. Let R be a ring, $e \in R$. We say e is idempotent if $e^2 = e$. We say e is central idempotent if further $e \in Z(R)$, namely $er = re$ for any $r \in R$. We say two idempotent e, f are orthogonal if $ef = fe = 0_R$. Let R has unit 1_R. Then the decomposition of 1_R into orthogonal idempotent $1_R = e_1 + e_2 + \cdots + e_n$ such that $e_ie_j = \delta_{ij}$.

Lemma 4. Suppose the idempotent decomposition are central and $e_i \neq 0$, then

$$R \cong Re_1 \times Re_2 \times \cdots \times Re_n$$

by $r \mapsto (re_1, re_2, \ldots, re_n)$.

Lemma 5. Let M, N two sides ideals of R such that $M \cup N = \{0\}$ and $M + N = R$, then there exists $(e_M, e_N) \in M \times N$ such that e_M, e_N are central idempotent in R and $R \mapsto Re_N \times Re_M$ by $r \mapsto (re_M, re_N)$ is an isomorphism of unitary ring.

Lecture 15-16 Mar 5,10

Topic: Introduction to Modules; Definition and Examples; Submodule.

Definition of Module

Definition 30. R is a ring (not commutative but unitary). M is an R-module (on the left) if $(M, +)$ is an abelian group and there exists $\varphi : R \to \mathrm{End}_{\text{group}}(M)$ as homomorphism of unitary rings.

Note. We often write: M is R-module via $R \times M \to M$ by $(r, m) \mapsto r \cdot m = \varphi(r)(m)$. Then we have the following: (1) $r(m + n) = rm + rn$; (2) $1_R \cdot m = m$ $[\varphi(1_R) = id]$; (3) $(r + s)m = rm + sm$ $[\varphi(r + s) = \varphi(r) + \varphi(s)]$; and (4) $(rs) = r(sm)$ $[\varphi(rs) = \varphi(r)\varphi(s)]$. This is a equivalent definition.

Example 35. Examples of Modules.

1. $R = k$ is a field. Then k-modules is just k-vector space.
2. $R = \mathbb{Z}$. Let $(M, +)$ be an abelian group. It is naturally a $\mathbb{Z}$-module since we have $\varphi : \mathbb{Z} \to \mathrm{End}_{\text{group}}(M)$ by $1 \mapsto id_M$ (and $2 \mapsto id_M + id_M$).
3. If k is a vector space and R is a k-algebra, then an R-module is a also a k-vector space. Since we can construct the following ring homomorphism

   rings

   $$k \longrightarrow R \xrightarrow{\varphi} \mathrm{End}_{\text{group}}(M)$$

   $$\lambda \mapsto \lambda \cdot 1_R$$

4. R is an R-module via $R \times R \to R$ by $(r, x) \mapsto rx$. Or we have the ring homomophism $\varphi : R \to \mathrm{End}_{\text{group}}(R)$ by $r \mapsto (r \mapsto rx)$. For example, $\mathbb{Z}$ is an $\mathbb{Z}$-module.
5. I ia a left ideal of R, then it is a (left) R-module via $R \times I \to I$ by $(r, x) \mapsto rx$.
6. V is a k-vector space. $R = \mathrm{End}_k(V) \subset \mathrm{End}_{\text{group}}(V)$. So V is an $\mathrm{End}_k(V)$-module via $\mathrm{End}_k(V) \times V \to V$ by $(f, v) \mapsto f(v)$.
7. $V = k^n$. $\mathrm{End}_k(V) \cong M_n(k)$ so k^n is a $M_n(k)$-module via $M_n(k) \times k^n \to k$ by $(A, v) \mapsto Av$.
8. R, S are rings and $\Psi : R \to S$ is a ring homomorphism. Let M be a S-module. Then it is a naturally an R-module via $R \times M \to M$ by $(r, m) \mapsto \Psi(r)m = \varphi(\Psi(r))(m)$. More simply it is just map composition: $\varphi \circ \Psi : R \xrightarrow{\Psi} S \xrightarrow{\varphi} \mathrm{End}_{\text{group}}(M)$.

9. k is field and V is a k-vector space. Pick $T \in \text{End}_k(V)$ where $\text{End}_k(V)$ is k algebra. Define $k[X] \to \text{End}_k(V)$ by $P(X) \mapsto P(T)$. We just endowed V with a structure of $k[X]$-module via T. This is because V is a $\text{End}_k(V)$ so by 8, it is a $k[X]$-module. Or more explicitly, we have $k[X] \times V \to V$ by $(P, v) \mapsto P(T)(v)$.

10. $V = k^n$. Pick a matrix $A \in M_n(k)$. V is a $k[X]$-module via A. More explicitly, we have $k[X] \times k^n \to k^n$ by $(P, v) \mapsto P(A)(v)$. We could study k^n as a $k[X]$-module and decide the statements about A.

11. In general, G is a group then G acts on set X if we have a group homomorphism $G \to \sigma(X)$ where $\sigma(X)$ is the set of bijections $X \to X$. Let k be a field and V is a k-vector space. Representation of G on V is a group homomorphism $\varphi : G \to \text{Aut}_k(V) = GL(V)$ where $GL(V) := (\text{End}_k(V))^\times$. It is a group action of G on V which satisfies $g(\lambda v + \mu w) = \lambda gv + \mu gw$. Let $R = k[G]$ a group ring of G over k. We can find a ring homomorphism $k[G] \to \text{End}_k(V)$ by $\sum_{\text{finite}} \lambda_i g_i \mapsto \sum_{\text{finite}} \lambda_i \varphi(g_i)$. So V is a $k[G]$-module via $(\sum \lambda_i g_i, v) \to \sum \lambda_i \varphi(g_i) v$. Vice verso, one can check that a $k[G]$-module can be seen on a representation of G over a k-vector space.
Example: G is a group and k is a field. Consider $\varphi : G \to k^\times = GL_1(k)$ by $g \mapsto 1$ a trivial map of G. This is a 1-dimensional representation of G over $V = k$. Set $V = k$ as a $k[G]$-module and we can find a homomorphism $k[G] \to \text{End}_k(k) = M_1(k) = k$ by $\sum \lambda_i g_i \mapsto \sum \lambda_i$

Submodules

Definition 31. If M is an R-module and $(N, +)$ is a subgroup of $(M, +)$, it is a (left) sub-R-module of M if $r \in R$, $n \in N$, we have $rn \in N$. [We can induce a group homomorphism $\varphi' : R \to \text{End}_{\text{group}}(N)$].

Example 36. Examples on Submodules.

1. R is an R-module, its submodules are left ideals.

2. R is a ring, I is a left ideal and M is an R-module. $IM := \left\{ \sum_{\text{finite}} x_i m_i, x_i \in I, m_i \in M \right\}$ is a subgroup of M. This is an sub-R-module of M.

3. Let $\mathcal{B} = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a, b, c \in k \right\} \subset \text{GL}_2(k)$. We have know that k^2 is a $k[\mathcal{B}]$-module via $k[\mathcal{B}] \times k^2 \to k^2$ by $(\sum \lambda_i A_i, v) \mapsto \sum \lambda_i A_i v$. Then we want to find the submodules of k^2. The trivial one is simply $\{0\}$. If it is not $\{0\}$, then it is a 1 dimensional vector space, We want to for any $A \in \mathcal{B}$, $A(\lambda_1 e_1 + \lambda_2 e_2) \in V$. Then it could be reduced back to an eigenvalue problem $Ab = kv$. We can pick $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. This restrict $v = ke_1$.

4. Let $V = k^3$ and we choose canonical basis. Let $T : V \to V$ represented in this basis as $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 1 \end{pmatrix}$. Consider V as a $k[X]$-module via T. We want to find the sub-$k[X]$-module of V. (1) Let $W = ke_1$. Let $P \in k[X]$ and $v \in W$. Then $Pv = P(T)ke_1 = k\sum a_i T^i(e_1) = k\sum a_i 2^i(e_1) = (k\sum a_i 2^i)e_i \in W$. (2) $U = k_2e_2 + k_3e_3$. Let $P \in k[X]$ and $v \in U$. Since $Te_2 \in U$ and $Te_3 \in U$, then $Pv = P(\lambda_2 e_2 + \lambda_2 e_3) = \lambda_2 P(T)e_2 + \lambda_3 P(T)e_3 \in U$. We see the key point is $T(U) \subset U$, namely U is stable by T.

Summary: (of 3 and 4) V is a k-vector space. $T \in \mathrm{End}_k(V)$. Consider V as a $k[X]$-module via T. Then we have

1. A sub-$k[X]$-module of V is a sub-vector space of V.
2. Let U be a sub-k-vector space of V. U is a sub-$k[X]$-modules of V if and only if $T(U) \subset U$, namely, U is stable by T.

Example 37. An exercise related to submodules. Consider $\mathcal{U} = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \middle| \, x \in k \right\}$ where $k = \mathbb{Z}/p\mathbb{Z}$. Show (a) $\mathcal{U} \cong \mathbb{Z}/p\mathbb{Z}$ as a group. (b) k^2 is naturally a $k[\mathcal{U}]$-module. What are its submodule?