Lecture 0 (04-01-2022)

04 January 2022 17:05

Text: T.Y. Lam - A First Course in Noncommutative Rings

Reference: R.S. Pierce - Associative Algebras

Grading: 2 Quizzes 10% each, Midsem 30%, Endsem 50%.

Ring → R with binary operations $+$, $\cdot$, and elements $0, 1 \in R$.

① $(R, +, 0)$ is an abelian group.

② $\cdot$ is associative.

③ $1 \cdot a = a \cdot 1 = a \quad \forall a \in R$.

④ $\left.\begin{array}{l} a \cdot (b + c) = a \cdot b + a \cdot c \\ (a + b) \cdot c = a \cdot c + b \cdot c \end{array}\right\} \forall a, b, c \in R$

($a \cdot b \neq b \cdot a$ is possible.)

Left ideal: $I \subseteq R$ is a left ideal if

① $0 \in R$,

② I is an additive subgroup of R,

③ $a \in R,\ i \in I \implies ai \in I$.

Right ideal: similar.

I is an ideal $:=$ I is a left and right ideal.

Left R-module: $(M, +, \cdot)$ is a left R-module

$+ : M \times M \to M, \quad \cdot : R \times M \to M$

① $(M, +)$ is an abelian group.

② $a \cdot (b \cdot m) = (ab) \cdot m \quad \forall a, b \in R \ \forall m \in M$

③ $1 \cdot m = m \quad \forall m \in M$

④ distributivity of both.

4 distributivity of both.

Lecture 1 (07-01-2022)

07 January 2022 17:30

$R \to$ Ring.

1. $Z(R)$ = center of R
$$= \{a \in R : ar = ra \ \forall r \in R\}$$ (Always a subring of R.)

2. $a \in R$ is a unit if $\exists b \in R$ s.t. $ab = 1 = ba$.

3. R is called a division ring if every $a \in R \setminus \{0\}$ is a unit and $1 \neq 0$. (Field if commutative, i.e., $R = Z(R)$.)

Examples. ① Hamiltonians (Quaternions)

$$\mathbb{H} \cong \mathbb{R}^4$$

(a, b, c, d)

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}.$$

$$i^2 = j^2 = k^2 = -1, \qquad ij = -ji = k.$$

$$\mathbb{R} \hookrightarrow \mathbb{H}$$
$$r \mapsto (r, 0, 0, 0)$$
$$Z(\mathbb{H}) = \mathbb{R}.$$

$$\alpha = a + bi + cj + dk,$$
$$\bar{\alpha} = a - bi - cj - dk.$$
$$\|\alpha\|^2 = \alpha \cdot \bar{\alpha} = a^2 + b^2 + c^2 + d^2.$$

$$\alpha \cdot \frac{\bar{\alpha}}{\|\alpha\|} = 1 \quad \text{for } \alpha \neq 0.$$

$\therefore$ $\mathbb{H}$ is a division ring (non commutative).

② Let k be a field.

$M_n(k)$ = $n \times n$ matrices over k.

$M_n(k)$ is NEVER commutative if $n \geq 2$ and k is arbitrary.

Check that $\begin{pmatrix} 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \end{pmatrix}$ do not commute.

$M_n(k)$ is NEVER commutative if $n \geq 2$ and k is arbitrary.

Check that $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ do not commute. $(0 \neq 1)$

In fact, given a commutative ring R, one can construct $M_n(R)$. This will again be non-comm for $n \geq 2$ if $R \neq 0$. One can even do this if R non-comm.

③ Let M, N be left R-modules.

$\mathrm{Hom}_R(M, N) = \{f : M \longrightarrow N \mid f \text{ is } R\text{-linear}\}$.

In general, $\mathrm{Hom}_R(M, N)$ is only an abelian group.

$$(f+g)(m) = f(m) + g(m).$$

If R is comm., we can define

$$(rf)(m) := r \cdot f(m).$$

But for non commutative, above definition may not be R-linear. Indeed, if $a \in R$, then we want

$$(rf)(am) = a((rf)(m)) = ar\,f(m).$$

OTOH, $(rf)(am) = f(ram) = ra \cdot f(m)$.

However, $\mathrm{Hom}_R(M, N)$ is an S-module for any subring $S \subseteq Z(R)$.

Def^n. $S \subseteq R$ is said to be a subring of R if
- S is an additive subgroup,
- S is a multiplicative submonoid (in particular, $1_R \in S$).

Example. $R = \mathbb{Z}/10\mathbb{Z}$.

$S = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$.

This is additive and multiplicatively closed.

Moreover, $\bar{6} \cdot x = x \quad \forall x \in S$.

Thus, $\bar{6}$ acts as a unit for S.

Thus, S is a ring BUT NOT A SUBRING OF R.

Remark. If $f: M \longrightarrow N$ is R-linear and $S \subseteq R$ a subring, then f is S-linear.

Example. $R = \mathbb{C}[x] \longrightarrow$ inf. dim. vspace over $\mathbb{C}$.

$\mathrm{Hom}_{\mathbb{C}}(\mathbb{C}[x], \mathbb{C}[x])$.

$$T = A_1(\mathbb{C}) = R\left\{ \begin{array}{ll} \mu_r : R \longrightarrow R, & \mu_r(t) = rt \,; r \in R \\ \frac{\partial}{\partial x} : R \longrightarrow R, & \frac{\partial}{\partial x}(f) = f' \end{array} \right\}.$$

$\hookrightarrow$ subring of $\mathrm{Hom}_{\mathbb{C}}(R, R)$ generated by $\mu_r \, (r \in R)$ and $\frac{\partial}{\partial x}$.

Bernstein: If M is an $A_1(\mathbb{C})$-module s.t. $\dim_{\mathbb{C}}(M) < \infty$, then $M = 0$.

Note: Over $R = \mathbb{C}[x]$, we can get nontrivial such modules. For example, $M_n = R/(x^n)$ is an R-module with $\dim_{\mathbb{C}}(M_n) = n < \infty$ and $M_n \neq 0$.

Proof. Let $\beta = \frac{d}{dx} \cdot \mu_x - \mu_x \cdot \frac{d}{dx}$.

Let $f \in \mathbb{C}[x]$.

Then,

$$\begin{aligned} \beta(f) &= \frac{\partial}{\partial x}(xf) - x\left(\frac{\partial}{\partial x} f\right) \\ &= f + x \cdot \frac{\partial f}{\partial x} - x \cdot \frac{\partial f}{\partial x} \\ &= f. \end{aligned}$$

$\therefore \beta = 1_{A_1(\mathbb{C})}$.

Suppose $\exists M \neq 0$ over $A_1(\mathbb{C})$ s.t. $\dim_{\mathbb{C}}(M) = n > 0$ with $n < \infty$.

Fix basis for M over $\mathbb{C}$.

$\mu_x : M \longrightarrow M$ is $\mathbb{C}$-linear. Let A be matrix rep.

$\frac{\partial}{\partial x} : M \longrightarrow M$ is also $\mathbb{C}$-linear. — " — B — " ——— .

Then, $BA - AB = I_{n\times n}$.

But taking trace gives a contradiction since $tr(AB) = tr(BA)$ but $tr(I_{n\times n}) = n \neq 0$. ∎

Recall: G is simple if $|G| \leq 59$ unless $G \cong \mathbb{Z}/p\mathbb{Z}$.

For $|G| = 60$, $G \cong A_5$ is precisely the non-simple group.

Groups of order p^n are not simple for $n \geq 2$.
(The center is normal and nontrivial.)

Burnside: $|G| = p^a q^b$, p, q prime, $a+b \geq 2 \Rightarrow G$ not simple.

Rep theory: Study of group homomorphisms $\rho : G \longrightarrow GL_n(\mathbb{C})$.

Emmy Noether: f.g. modules over $\mathbb{C}[G]$ $\equiv$ Group rep of G.

Group rings $k[G]$
- modular case: $|G| = 0$ in k
- non modular case: $\frac{1}{|G|} \in k$.

Def^n. Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group, and k a field.

$k[G] := kg_1 \oplus kg_2 \oplus \cdots \oplus kg_n$.

Addition is defined component wise.

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{g\in G} b_g g\right) = \sum_{g\in G}\left(\sum_{\sigma\tau = g} a_\sigma b_\tau\right) g.$$

EXAMPLE. $G = S_3 = \{1, a, a^2, b, ab, a^2b\}$, $a^3 = b^2 = 1$, $ba = a^2 b$.

$k = \mathbb{Q}$.

$\alpha = 2 + 3a + 4b + 5a^2b$,

$\beta = a + 2b$.

Then, $\alpha\beta = (2 + 3a + 4b + 5a^2b)(a + 2b)$

$= 2a + 3a^2 + 4ba + 5a^2ba$

$+ 4b + 6ab + 8b^2 + 10a^2b^2$

$= 2a + 3a^2 + 4a^2b + 5ab + 4b + 6ab + 8 + 10a^2$

$= 8 + 2a + 13a^2 + 4b + 11ab + 4a^2b.$

Let k be a field. Let G act on k, i.e., $G \to \mathrm{Aut}(k)$ is a homom.

$$k^G = \{a \in G : \sigma(a) = a \quad \forall \sigma \in G\}.$$

Artin:

$$\begin{array}{c} k \\ | \\ k^G \end{array} \quad \text{finite normal sep ext}^n \text{ of } k^G.$$

- $R = k[x_1, \dots, x_n]$.

$G \leq GL_n(k)$ finite.

G acts on R. R^G is a subring. (Hilbert showed this is Noetherian!)

Defn. Let G be a finite group.

Let R be a ring.

Let $\rho : G \to \mathrm{Aut}(R)$ be a group homomorphism.

Define the skew group ring $R *_\rho G$ as follows:

$$R *_\rho G = \left\{ \sum_{g \in G} r_g \cdot g \ : \ r_g \in R \right\}.$$

$$(a_\sigma \sigma) \cdot (b_\tau \tau) := a_\sigma \, \rho(\sigma)(b_\tau)\,(\sigma\tau)$$

(Basically: $g \cdot r := \rho(g)(r)$.)

Lecture 2 (11-01-2022)

11 January 2022 17:30

Convention: A module by default means "left module".
The definitions are analogous for right modules.

Def^n An R-module M is said to be simple if
- $M \neq 0$,
- $N \leq M \Rightarrow N = 0$ or $N = M$.

N is an R-submodule of M

Q. Are simple modules f.g.?
Yes. Pick any $m \in M \setminus \{0\}$. Then, $\langle m \rangle = M$.

EXAMPLES

1) $k \to$ field. $(R = k)$

If M is a f.g. k-module, then M is a f.dim k-vec space.
Thus, $M \cong k^n$.
In particular, M is simple $\Leftrightarrow M \cong k$.
There is only one simple module!

2) $R = M_n(k)$
$\cong \mathrm{Hom}_k(k^n, k^n)$. $(n = 1 \uparrow)$

Assume $n \geq 2$. Note: R is noncommutative for any choice of k.
e.g.: for $n=2$, consider $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

We have $k \cong Z(R)$ by $a \mapsto a I_{n \times n}$.

Let $V = k^n$ as column vectors.

$$= \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} : a_i \in k \right\}.$$

R acts on V by left multiplication.

Lemma. V is a simple R-module.

Proof. Pick $0 \neq v \in V$. To show: $\langle v \rangle = V$.

Extend $\{v\}$ to a k-basis $\{v = v_1, v_2, \ldots, v_n\}$ of V.

For each $i \in [n]$, we can find a matrix $A_i \in R$ s.t.

$$A_i v = v_i.$$

(Think in terms of linear transformation by sending all the basis elements to v_i)

Thus, $v_1, \ldots, v_n \in \langle v \rangle$.

Note that $\langle v \rangle$ is also a k-vec space.

$\therefore$ all k-linear combinations of $v_1, \ldots, v_n$ are in $\langle v \rangle$.

$\therefore V \subseteq \langle v \rangle$. ∎

will prove later.

FACTS: ① V is the unique simple R-module.

② M is any f.g. left R-module $\Rightarrow$ $M \cong V \oplus \cdots \oplus V$.

Again, unique simple module!

3) $R = \mathbb{Z}$.

$\mathbb{Z}/p\mathbb{Z}$ is simple for all primes $p \geq 2$.

Infinitely many simple modules this time!

Theorem. Let R be a ring such that $k \hookrightarrow Z(R)$.

Assume that $\dim_k(R) < \infty$.

Then, there are only finitely many simple R-modules.

Proof Later. ∎

4) $T_n(k) :=$ $n \times n$ upper triangular matrices over k.

$$\begin{aligned} k &\hookrightarrow Z(T_n(k)) \\ a &\longmapsto a I_{n \times n}, \end{aligned} \qquad \dim_k T_n(k) < \infty.$$

Define the R-modules $V_1, \dots, V_n$ as follows:
$V_i \cong k$ as k-vector spaces.

The action on V_i is as follows:

$$\begin{pmatrix} a_{11} & * & * \\ & \ddots & * \\ 0 & & a_{nn} \end{pmatrix} \cdot x := a_{ii} x.$$

(Multiplication by a_{ii}. Check that above is indeed a module.)

Propn. $V_1, \dots, V_n$ are all distinct simple R-modules.

Proof Simplicity is clear since $\dim_k (V_i) = 1$.
Now, let $1 \leq i < j \leq n$ be given. Let

$$f : V_i \to V_j$$

be an R-linear map. We show that $f = 0$. In particular, there is no R-linear isomorphism from V_i to V_j.
Let $x \in V_i$.
Consider the element $A = E_{ii}$. ← 1 in (i,i), 0 else
Then, $x = A \cdot x$.
Applying f gives

$$\begin{aligned} f(x) &= f(A \cdot x) \\ &= A \cdot f(x) \quad \text{in } V_j \\ &= 0. \end{aligned}$$

∎

$= A \cdot f(x)$ in V_j

$= 0.$ ∎

Theorem (Schur's lemma) Let M, N be simple modules.

(i) $\mathrm{Hom}_R(M, N) = 0$ if $M \not\cong N$.

(ii) $\mathrm{Hom}_R(M, M)$ is a division ring.

Proof. We show that if $f: M \to N$ is nonzero, then it is an isomorphism. Both parts follow at once.

$f \neq 0 \Rightarrow \ker(f) \neq M \Rightarrow \ker(f) = 0$ since M is simple.

$\Downarrow$

f is one-one.

$f \neq 0 \Rightarrow \mathrm{im}(f) \neq 0 \Rightarrow \mathrm{im}(f) = N$ since N is simple

$\Downarrow$

f is onto. ∎

x x

EXAMPLES SO FAR: ① $R_1 = \mathbb{R}$.

② $R_2 = M_n(\mathbb{R}) = \mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R}^n)$.

③ $R_3 = \mathbb{Z}$.

④ $R_4 = \mathcal{I}_n(\mathbb{R})$.

EXAMPLE 5. $V = \mathbb{R}^n$.

$\mathrm{Hom}_{\mathbb{R}}(V, V) \cong R_2$. (1)

Note that V is also an R_2-module.

Claim $\mathrm{Hom}_{R_2}(V, V) \cong \mathbb{R}$. ((Compare with (1)!) The map constructed will also be a ring isomorphism!

(Iso. as $\mathbb{R}$-vec spaces. Recall that Hom is a $Z(R)$-module.)

Proof. $\Psi: \mathbb{R} \longrightarrow \mathrm{Hom}_{R_2}(V, V)$.

$a \longmapsto \varphi_a$, where $\varphi_a : V \longrightarrow V$ is

$u \longmapsto a \cdot u$.

Easy to see that Ψ is well-defined, $\mathbb{R}$-linear, and one-one.

Onto:

Step 1. Let $f: V \to V$ be R_2-linear.

Let $\{e_1, \dots, e_n\}$ be the standard k-basis for V.
Define $v_i := f(e_i)$.

Step 2. For all i: $\{e_i, v_i\}$ is lin. dep.

Proof. Suppose they are lin. indep for some i.
Can find $A \in R_2$ s.t. $Av_i = e_i$ and $Ae_i = 0$.

$$\begin{array}{c} f(Ae_i) = A \cdot f(e_i) = Av_i = e_i. \\ \shortparallel \\ 0 \end{array}$$

$\rightarrow\leftarrow$

Step 3. By Step 2, $\exists\, \alpha_1, \dots, \alpha_n \in k$ s.t. $v_i = \alpha_i e_i$ $\forall i \in [n]$.
Suffices to show that all α_i are same.

Let $i \neq j$. Pick a perm. matrix $P \in R_2$ s.t.
$Pe_i = e_j$, $Pe_j = e_i$.

$$\begin{aligned} \alpha_i e_i = v_i = f(e_i) = f(Pe_j) &= P f(e_j) \\ &= P v_j \\ &= \alpha_j P e_j = \alpha_j e_i. \end{aligned}$$

$\therefore \alpha_i = \alpha_j$. ∎

Opposite Ring : R^{op}

- Let $(R, +, \cdot)$ be a ring.
- As an abelian group, $(R^{op}, +) = (R, +)$.

Multiplication is defined as

$$\underset{\text{in } R^{op}}{a \cdot b} := ba.$$

- $R \to$ ring. $S := \mathrm{Hom}_R(M, M) = \mathrm{End}_R(M)$ is a ring with multiplication being composition.

- $\mathrm{Hom}_R(R,R) \cong R^{op}$ as rings.
  $f \longmapsto f(1)$

$$\begin{tikzcd} M \arrow[r, "g"] \arrow[dr, "fg"'] & M \arrow[d, "f"] \arrow[dl, phantom, "\circlearrowright"] \\ & M \end{tikzcd}$$

- More generally,

$$\mathrm{Hom}_R(R^n, R^n) \cong M_n(R^{op}).$$

(In particular, R comm $\Rightarrow$ $\mathrm{Hom}_R(R^n, R^n) \cong M_n(R)$,
$\mathrm{Hom}_R(R, R) \cong R$.)

- Let M be a LEFT R-module.
  Then, M is a RIGHT S-module. ($S := \mathrm{Hom}_R(M,M)$.)

$$m \cdot f := f(m).$$

M is an R-S-bimodule.

Proof. $\Psi : \mathrm{Hom}_R(R^n, R^n) \longrightarrow M_n(R^{op})$.

$$f \longmapsto \begin{bmatrix} | & | & & | \\ f(e_1) & f(e_2) & \cdots & f(e_n) \\ | & | & & | \end{bmatrix}.$$

$$\Psi(fg) = \begin{bmatrix} | & & | \\ fg(e_1) & \cdots & fg(e_n) \\ | & & | \end{bmatrix}.$$

$$\Psi(f)\Psi(g) = \begin{bmatrix} | & \\ f(e_1) & \cdots \\ | & \end{bmatrix}\begin{bmatrix} | & \\ g(e_1) & \cdots \\ | & \end{bmatrix}$$

Lecture 3 (13-01-2022)

13 January 2022 15:26

(1) $R_1 = k \to$ field.

M f.g. over $k \iff M \cong k^n$.

k is the unique simple module over R_1.

(2) $R_2 = M_n(k)$, $V = k^n \longleftrightarrow$ unique simple R_2-module.

(Will show: f.g. modules over R_2 are $V \oplus V \oplus \cdots \oplus V$)

(3) $R_3 = \mathbb{Z}$.

For each prime p, $\mathbb{Z}/p\mathbb{Z}$ is a simple $\mathbb{Z}$-module.

(In particular, there are infinitely many!)

(4) $R_4 = T_n(k) \to$ upper triangular matrices

$V_i = ke_i$. $V_i \not\cong V_j$ for $1 \leq i < j \leq n$.

Defn. $R \longrightarrow$ ring

$M \to$ (left) R-module

We say that M is Noetherian if every ascending chain of submodules of M stabilises.

Exercise TFAE:

(i) M is Noetherian.

(ii) Every nonempty collection of submodules of M has a maximal element.

Defn. $0 \to N \xrightarrow{\alpha} E \xrightarrow{\beta} L \to 0$ is said to be a short exact sequence of left R-modules if

(i) α is one-one,

(ii) $\mathrm{im}(\alpha) = \ker(\beta)$,

(iii) β is onto.

Exercise: Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be a s.e.s.
TFAE:

(i) M_2 is Noe.
(ii) M_1 and M_2 are Noe.

Note: R has two obvious structures as an R-module.
As a left module, we write ${}_R R$ and as a right we write R_R.

Def^n. R is said to be left Noetherian if ${}_R R$ is Noetherian.
(Similarly for right.)

Note: There exist (necessarily noncommutative) rings which are left Noetherian but not right.

Dual condition of Noetherian: Artinian (descending chains stabilize).
Similarly, a ring is left (resp. right) Artinian if it Artinian as a left (resp. right) module over itself.

Remark: Again left Artinian $\not\Rightarrow$ right Artinian $\not\Rightarrow$ left Art.

Hopkin-Levitzki: ${}_R R$ Artin $\Rightarrow$ ${}_R R$ Noetherian.
R_R Artin $\Rightarrow$ R_R Noetherian.

Examples. • $\mathbb{Z}$ is Noetherian but not Artinian. Thus, converse of above is not true.

• $k \hookrightarrow R$ s.t. • $k \subseteq Z(R)$,
• $\dim_k(R) < \infty$.

Then, R is left Artin and left Noe.

Then, R is left Artin and left Noe.
(Any left ideal is a k-vector space...)

did not REALLY require this for this example
(Then we would talk about dim as left/right k-vec space.)

- Every PID (or more generally PIR) is Noetherian.
  Every ID which is not a field is not Artin. Take $a \in R \setminus \mathcal{U}(R)$, then
$$aR \supsetneq a^2R \supsetneq a^3R \supsetneq \cdots$$

- $R = k[x_1, x_2, x_3, \ldots]$.
  $(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots$ NOT Noe.
  $(x_1) \supsetneq (x_1^2) \supsetneq (x_1^3) \supsetneq \cdots$ NOT Artinian.

Question: When is an (left) R-module both Artinian and Noetherian?

Def^n. We say that a left R-module M has a composition series

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$$

if M_{i+1}/M_i is a simple (left) R-module for all $i \in \{0, \ldots, n-1\}$.

Theorem. TFAE:
(i) M is Artinian and Noetherian.
(ii) M has a composition series.

Proof. (ii) $\Rightarrow$ (i)

Observation: E simple $\Rightarrow$ E is Art + Noe.

M_1, M_2/M_1 are simple $\Rightarrow$ M_1, M_2/M_1 are A + N
$\Downarrow$

M_2 is A + N.

Then consider $0 \to M_2 \to M_3/M_2 \to M_3 \to 0$ and so on.

(i) $\Rightarrow$ (ii) Assume $M \neq 0$.

$\mathcal{C}_1 := \{ N : N \subsetneq M \}$.

$0 \in \mathcal{C}_1$. $\therefore \mathcal{C}_1 \neq \emptyset$.

By Noe., pick $M_1 \in \mathcal{C}_1$ maximal.

- $M_1 \subsetneq M$
- M/M_1 is simple.

If M_1 is simple, then we are done.

Else take $\mathcal{C}_2 := \{ N : N \subsetneq M_1 \}$ and keep going on to get

$$M \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots.$$

Since M is Art, this process must terminate and we are done. ∎

Lecture 4 (18-01-2022)

18 January 2022 17:26

- Artin + Noether $\Leftrightarrow$ $\exists$ composition series
- $k \hookrightarrow Z(A)$, $\dim_k A < \infty \Rightarrow A$ is both left Artin and Noe.

Recalling the proof of Jordan-Hölder, one similarly has:
Any two composition series (if they exist) are of same length, and the quotients appearing are permutations of each other.

Corollary. $k \hookrightarrow Z(A)$, $\dim_k(A) < \infty$.
There are only finitely many simple A-modules (up to isomorphism).

Proof. M simple $\Rightarrow$ $M \cong A/\mathfrak{q} \leftarrow$ simple.

$$A \supsetneq \mathfrak{q} \supsetneq \mathfrak{q}_r \supsetneq \cdots \supsetneq \mathfrak{q}_1 \supsetneq 0.$$

Thus, $A/\mathfrak{q}$ is a module appearing as one of the finitely many quotients in a comp. series of A.

- **Bimodule:** R, S ring.
  $M \longrightarrow (R\text{-}S)$-bimodule, denote ${}_R M_S$.
  $\hookrightarrow$ left R-module
  $\hookrightarrow$ right S-module

$$r\cdot(m\cdot s) = (r\cdot m)\cdot s \quad \forall r \in R,\ s \in S.$$

- Triangular rings.

Let R, S, ${}_R M_S$ be given. Define

$$A := \left\{ \begin{pmatrix} r & m \\ & s \end{pmatrix} : r \in R,\ m \in M,\ s \in S \right\}$$

$$A := \left\{ \begin{pmatrix} r & m \\ & s \end{pmatrix} : r \in R,\ m \in M,\ s \in S \right\}$$

$$\equiv \begin{pmatrix} R & M \\ & S \end{pmatrix}.$$

A is a ring with obvious addition and multiplication as

$$\begin{pmatrix} r & m \\ & s \end{pmatrix} \cdot \begin{pmatrix} r' & m' \\ & s' \end{pmatrix} = \begin{pmatrix} rr' & rm' + ms' \\ & ss' \end{pmatrix}.$$

	R	M	S
R	R	M	0
M	0	0	M
S	0	0	S

Proposition. (Self-study)

① Left ideals of A are of the form $I_1 \oplus I_2$, I_2 is a left ideal in S, I_1 is a left R-submodule of $R \oplus M$ containing MI_2.

② Right ideals of A are of the form $J_1 \oplus J_2$, where J_1 is a right ideal in R, and J_2 is a right S-submodule of $M \oplus S$ containing $J_1 M$.

Corollary. $\begin{pmatrix} \mathbb{C} & \mathbb{C} \\ & \mathbb{Q} \end{pmatrix}$ is left-Noe. and left Artin but NOT right-Art nor right-Noe. $(\dim_{\mathbb{Q}} \mathbb{C} = \infty.)$

Recall: Let V be a f.d. k-vec. space.
Let $f : V \to V$ be k-linear.
Then, f is one-one $\Leftrightarrow$ f is onto.
The above is false if $\dim_k(V) = \infty$. (Consider the shift-operators.)

Defn. ① A ring R is Dedekind-finite if:

$\forall a, b \in R : ab = 1 \Rightarrow ba = 1.$

② $a \in R$ is called a left zerodivisor if $a \neq 0$ and $\exists b \neq 0$ s.t. $ab = 0$.

③ $R^{\neq 0}$ is called a domain if $ab = 0 \Rightarrow a = 0$ or $b = 0$ $\forall a, b \in R$.

④ R is called reduced if $a^n = 0 \Rightarrow a = 0$ $\forall a \in R$ $\forall n \in \mathbb{N}$.

EXAMPLES.

(1) $k \to$ field, $\sigma : k \to k$ field endomorphism (not necessarily onto)

HILBERT TWIST.

$$k[x, \sigma] := \left\{ \sum_{\text{finite sum}} a_n x^n : a_n \in k \right\}.$$

Addition is usual.

$$x \cdot a := \sigma(a)\, x.$$

(i) $\sigma \neq id \Rightarrow k[x, \sigma]$ is not commutative.

(ii) left polynomials $\{\sum a_i x^i\}$

right polynomials $\{\sum x^i b_i\}$

If σ is not onto, then not all left polynomials are also right polynomials.

· Similarly, can do this with power series to get $k[[x, \sigma]]$.

· $$k((x)) = \left\{ \sum_{a_r = 0} a_r x^r : a_r \in k \right\} = \text{Laurent series.}$$

for $r<<0$

Can talk about $k((x\,;\,\sigma))$. Here, one takes $\sigma \in \mathrm{Aut}(k)$.

$k = \mathbb{Q}(t)$. $\sigma : t \longmapsto 2t$.

$k((x\,;\,\sigma))$ is a division ring.

(2) Let G act on a ring A by automorphisms.

$$A * G = \left\{ \sum_{\sigma \in G} a_\sigma \sigma \;:\; a_\sigma \in A,\ \sigma \in G \right\}.$$

Addition component wise. Multiplication:

$$(a\sigma) \cdot (b\tau) = \underbrace{a \cdot \sigma(b)}_{\in R}\ \underbrace{(\sigma\tau)}_{\in G}.$$

3) $k[G] \longrightarrow$ group ring, G finite group.

Algebras.

- $A \longrightarrow$ commutative ring.

$R \longrightarrow$ ring.

R is said to be an A-algebra via φ if $\varphi : A \longrightarrow Z(R)$ is a ring homomorphism.

Example. $k \hookrightarrow A$, $i(k) \subseteq Z(A)$, $\dim_k A < \infty$.

$\operatorname{Hom}_k(A, k) \longrightarrow$ injective A-module

$\hookrightarrow$ f.g. as an A-module

$\operatorname{mod}(A) = \{M : M$ is a f.g. left A-module$\}$

has proj. + inj. modules in this case.

Lecture 5 (21-01-2022)

21 January 2022 17:22

Semisimplicity

Recall: A left R-module M is called simple if
$M \neq 0$ and $N \leq M \implies N = 0$ or $N = M$.

Defn. M is semisimple if for every submodule $N \leq M$, there exists a submodule $K \leq M$ such that $M = N \oplus K$.
(Usual internal direct sum.)

Examples
1. 0 module is semisimple.
2. Every simple module is semisimple. $(M = M \oplus 0 = 0 \oplus M)$
3. Any (finite dimensional) vector space is semisimple.
   ↳ Can extend basis, assuming AoC.
4. $0 \to U \to V \to W \to 0$ s.e.s.
   V semisimple $\underset{\not\Leftarrow}{\Rightarrow}$ U, W are semisimple

Proof $(\Rightarrow)$ Let $K \leq U$. Then, $K \leq V$.
Write $V = K \oplus K'$.
Check: $U = K \oplus (K' \cap U)$.

Write $V = U \oplus U'$. Then, $W \cong U' \leq V$.
$\therefore$ W is semisimple by first part.

$(\Leftarrow)$ Take $R = \dfrac{k[x]}{(x^2)}$. $\rightsquigarrow$ commutative ring!

$$0 \longrightarrow (x) \longrightarrow R \longrightarrow R/(x) \longrightarrow 0.$$

↳ simple since isomorphic to k

Claim: R is not semisimple.
We show that (x) does not have a complementary submodule.

Indeed, if possible, assume that $R = (x) \oplus W$.
Since $(x) \neq R$, $W \neq 0$.
Let $t = ax + b \in W$.
Since $W \cap (x) = 0$, we have $b \neq 0$.
But then, $1 + \dfrac{ax}{b} = \dfrac{t}{b}$.

But then, $1 + \frac{ax}{b} = \frac{t}{b}$.

$\hookrightarrow$ nilpotent

$\therefore$ $\frac{t}{b}$ is a unit. But then $t^{\in W}$ is a unit.

But W is a proper ideal. $\boxtimes$

Def^n. R is said to be left semisimple as a ring if any f.g. R-module is semisimple.

Remark! We will show that R is left s.s. as a ring iff R is s.s. as a left R-module. In fact, in such a case, EVERY R-module is a semisimple module! (See Remark 2.)

Theorem! Let $R = k[G]$. ($k \to$ field, $G \to$ finite group)

R is semisimple $\Leftrightarrow$ $\frac{1}{|G|} \in k$.

$\Leftrightarrow$ $\mathrm{char}(k) \nmid |G|$.

Proof ($\Leftarrow$) Let V be a f.g. R-module (also a f.g. k-v.space). Let $0 \subsetneq W \subsetneq V$ ($k[G]$-submodule!).

We show that $\exists h : V \to W$ $k[G]$-linear s.t.

$$h(w) = w \quad \forall w \in W.$$

(That is, $0 \to W \rightleftarrows V \to V/W \to 0$ splits.)

This directly gives $V = W \oplus \ker h$.

Let $\{w_1, \ldots, w_r\}$ be a basis of W extended to $\{w_1, \ldots, w_r, t_1, \ldots, t_s\}$ of V.

Define the k-linear map $f: V \to W$ by

$$w_i \mapsto w_i,$$
$$t_j \mapsto 0.$$

Then, $f|_W = id_W$.

Define $h: V \to W$ by

$$h(v) = \frac{1}{|G|} \sum_{\sigma \in G} \sigma^{-1} f(\sigma v).$$

Then,

$$h(w) = \frac{1}{|G|} \sum_{\sigma \in G} \sigma^{-1} f(\sigma w)$$

$\sigma w \in W$ since w is a $k[G]$-submodule

$$= \frac{1}{|G|} \sum_{\sigma \in G} \sigma^{-1}(\sigma w)$$

$$= \frac{1}{|G|} \sum_{\sigma \in G} w = w.$$

Lastly, we wish to show that h is $k[G]$-linear.
Since it is k-linear, suffices to show that $h(gv) = gh(v)$ $\forall g \in G$.

$$h(gv) = \frac{1}{|G|} \sum_{\sigma \in G} \sigma^{-1} f(\sigma g v)$$
$$= \frac{1}{|G|} \sum_{\sigma \in G} g \cdot g^{-1} \sigma^{-1} f((\sigma g) v)$$
$$= \frac{1}{|G|} \sum_{\tau \in G} g \cdot \tau^{-1} f(\tau v)$$
$$= g \cdot \left(\frac{1}{|G|} \sum_{\tau \in G} \tau^{-1} f(\tau v) \right) = g \cdot h(v).$$

($\Rightarrow$) Later, when we study radicals ∎

Q. How to construct semisimple modules?

Theorem 2. Let M be a left R-module.
TFAE:
① M is semisimple.
② M is a sum of simple R-submodules.
③ M is a direct sum of simple R-modules.

Before proof, some examples.

Cor. k field $\Rightarrow M_n(k)$ semisimple as a module over itself.

Proof. Recall that $V \cong k^n$ is a simple $M_n(k)$-module.
Thus, $M_n(k) \cong \underbrace{V \oplus \cdots \oplus V}_{n}$ is semisimple. ∎

Cor. ${}_R R$ semisimple $\Rightarrow$ any R-module is simple.

Proof. Let M be any R-module. Map a free module $F = \bigoplus_I R$ onto M.
F is semisimple by Theorem 2.
M is a quotient of F and hence, semisimple by Example ④. ∎

Remark 2. The above reconciles Remark 1.
That is, TFAE:
(i) R is semisimple as a ring.
(That is, every f.g. R-module is a semisimple R-module)
(ii) R is semisimple as a left R-module.
(Note: R is f.g. over itself.)
(iii) Every R-module is semisimple.

Lemma. Let $M \neq 0$ be a semisimple module.
Then, N has a simple submodule.
(In particular, if $K \leq M$ is a nonzero submodule, then K has a simple submodule.)

Proof. Let $0 \neq m \in M$. $Rm \leq M$ is nonzero.
Can assume $Rm = M$.
Let

$$\mathcal{C} = \{K \leq M : m \notin K\}.$$

$\{0\} \in \mathcal{C}$ and thus, $\mathcal{C} \neq \emptyset$. Partially order $\mathcal{C}$ by $\subseteq$.

Let $\{K_\alpha\}$ be a chain in $\mathcal{C}$. Then, $\bigcup_\alpha K_\alpha$ is a submodule of M not containing m.
Thus, by Zorn's lemma, $\mathcal{C}$ has a maximal element, say T.

By semisimplicity, $M = T \oplus K$. Then K is simple. ∎

Proof of Thm 2:
(1) $\Rightarrow$ (2) Let M_0 = sum of all simple submodules of M.
If $M_0 \neq M$, then $M = M_0 \oplus K$ for some $K \neq 0$.
But K has a simple submodule then.
$\therefore K \cap M_0 \neq 0$. $\rightarrow\leftarrow$

(2) $\Rightarrow$ (1) $M = \sum_{i \in I} M_i$. Let $N \leq M$ be given.

$$\mathcal{C} = \left\{ J \subseteq I : \begin{array}{ll} (1) & \sum_{i \in J} M_i = \bigoplus_{i \in J} M_i \\ (2) & N \cap \left(\sum_{j \in J} M_j\right) = 0 \end{array} \right\}.$$

$\emptyset \in \mathcal{C}$. Partially order $\mathcal{C}$ by $\subseteq$.
Usual Zorn shows that $\mathcal{C}$ has a maximal J_0.

Let $K = \bigoplus M_j$. Clearly, $N \cap K = 0$.

Let $K = \bigoplus_{j \in J_0} M_j$. Clearly, $N \cap K = 0$.

Let $M' = N \oplus K$. We show $M = M'$!
If not, then $M_i \not\subseteq M'$ for some $i \in I$.
(Necessarily $i \notin J_0$.)
Then, $M' \cap M_i = \{0\}$ since M_i simple.
But the $J_0 \cup \{i\} \in \mathcal{C}$, contradicting maximality.

(2) $\Rightarrow$ (3) Same proof as above works with $N = 0$, since we produced a complement which was a direct sum of simple modules

Lecture 6 (28-01-2022)

28 January 2022 17:28

- Recall that for an R-module M, TFAE:
  1. M is semisimple.
  2. M is a sum of simple submodules.
  3. M is a direct sum of simple modules.

1. We also showed that if $\mathrm{char}(k) \nmid |G|$, then $k[G]$ is semisimple. Converse is true as well. (We did not show this.)

2. $R = M_n(k)$ is simple, $R = \bigoplus_{i=1}^{n} k^n$.

3. R is semisimple as a ring $\overset{\text{def}^n}{\iff}$ every f.g. R-module is semisimple
$\iff$ R is semisimple as a (left) module.
$\iff$ every R-module is semisimple.

Q. If R is semisimple as a left module, is it also semisimple as a right module? As we shall see, yes!

Thm (Artin-Wedderburn)
Let $R \neq 0$ be a ring. TFAE
(i) R is a left semisimple ring.
(ii) $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$, where D_i are division rings.
as rings $(r, (n_1, D_1), \ldots, (n_r, D_r))$ is an invariant of R.
(iii) R is a right semisimple ring.

Recall R^{op}.

Left R-module $\equiv$ Right R^{op} - module.

$$\left.\begin{aligned} a \cdot m &\longleftrightarrow m \cdot a \\ a \cdot (b \cdot m) &\longleftrightarrow (m \cdot b) \cdot a \\ a \cdot b &\longleftrightarrow b \cdot a \end{aligned}\right\} \begin{aligned} &a, b \in R \\ &m \in M \end{aligned}$$

EXAMPLE. $D \to$ Division ring.

Let $R = M_n(D)$, $V = D^n$. V is an R-module naturally.

Then,

1. R is semisimple.
2. ${}_R R \cong \underbrace{V \oplus \cdots \oplus V}_{n \text{ copies}}$.
3. $\mathrm{End}_R(V) \cong D^{op}$.

Proof of 3. Let $\mu_a : D^n \to D^n$ denote multiplication ON THE RIGHT by $a \in D$.

Define $\phi : D^{op} \to \mathrm{Hom}_R(D^n, D^n)$ by

$$a \mapsto \mu_a.$$

Then, ϕ is 1-1 and onto. (We had seen this for fields in lecture 2 Example 5.)

(Same proof goes.)

$\phi(1) = 1$. ✓

Now,
$$\phi(a \cdot b) = \mu_{a\cdot b} = \mu_{ba} = \mu_a \circ \mu_b = \phi(a) \circ \phi(b).$$ ∎

MULTIPLY ON THE RIGHT!

$\phi(a+b) = \phi(a) + \phi(b)$ is clearly true.

Theorem. $R_1, \ldots, R_n$ semisimple $\Rightarrow$ $R_1 \times \cdots \times R_n$ semisimple.

Proof. Suffices to show this for $n = 2$.

Write $R = \bigoplus_i U_i$, $S = \bigoplus_j V_j$.

Check $R \times S = \left(\bigoplus_i U_i \times S\right) \oplus \left(\bigoplus_j R \times V_j\right)$. ∎

EXERCISE. ① U simple R-module $\Rightarrow$ $U \times S$ is a simple $(R \times S)$-module.

② V simple S-module $\Rightarrow$ $R \times V$ is a simple $(R \times S)$-module.

Proof of Artin-Wedderburn :

① $\Rightarrow$ ②. Let R be left semisimple.

Write $R = \bigoplus_{i \in \Lambda} U_i$ for $U_i \subseteq R$ simple left ideals.

$$1 \in U_{i_1} \oplus \cdots \oplus U_{i_s}.$$

$$\Rightarrow \quad r = r.1 \in U_{i_1} \oplus \cdots \oplus U_{i_s} \quad \text{for all } r \in R.$$

$$\therefore \quad R = \bigoplus_{i=1}^{s} U_i \quad : \quad U_i \text{ simple.}$$

$$= \bigoplus_{i=1}^{r} V_i^{\oplus n_i} \quad : \quad V_i \text{ simple, } n_i \in \mathbb{N}, \quad r \geq 1,$$

$V_i \not\cong V_j$ for $i \neq j$.

$$R^{op} \cong \mathrm{Hom}_R(R, R) = \mathrm{Hom}_R\left(\bigoplus_{i=1}^{r} V_i^{n_i}, \bigoplus_{j=1}^{r} V_j^{n_j}\right)$$

$$\cong \bigoplus_{i,j} \mathrm{Hom}_R\left(V_i^{n_i}, V_j^{n_j}\right)$$

$$\cong \bigoplus_{i,j} \mathrm{Hom}_R(V_i, V_j)^{n_i n_j}$$

Schur

$$\cong \bigoplus_{i=1}^{s} \mathrm{Hom}_R\left(V_i^{n_i}, V_i^{n_i}\right)$$

$$= \prod_{i=1}^{s} \mathrm{End}_R\left(V_i^{n_i}\right).$$

$$\mathrm{Hom}_R\left(V_i^{n_i}, V_i^{n_i}\right) \cong \mathrm{Hom}_R(V_i, V_i)^{n_i^2}$$

$$\cong M_{n_i}(D_i).$$

$D_i := \mathrm{Hom}_R(V_i, V_i)$ check

div ring by Schur

Thus, $R^{op} \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$.

$$\Rightarrow \quad R \cong M_{n_1}(D_1^{op}) \times \cdots \times M_{n_r}(D_r^{op}).$$

Other directions now follow.

Proof also shows uniqueness : The V_i are characterised by the modules appearing in any Jordan-Hölder decomposition. So are the n_i. ∎

Lecture 7 (01-02-2022)

01 February 2022 17:36

Last time, we charactarised semisimple rings.

Thm. Let R be a ring. TFAE:

(i) R is left semisimple.

(ii) $R \cong \prod_{i=1}^{s} M_{n_i}(D_i)$.

(iii) R is right semisimple.

Semisimple ring $\equiv$ homological dim 0.

Def^n. A left R-module P is called *projective* if for every diagram

$$\begin{tikzcd} & P \arrow[d, "\beta"] & \\ N \arrow[r, "\alpha"'] & M \arrow[r] & 0, \end{tikzcd}$$

(α is onto)

there exists $h : P \to N$ s.t. $\alpha \circ h = \beta$.

$$\begin{tikzcd} & P \arrow[d] \arrow[dl, dashed, "\exists"] & \\ N \arrow[r] & M \arrow[r] & 0 \end{tikzcd}$$

EXAMPLES. Any free R-module is projective.

Prop^n. Any direct summand of a free module is projective. That is, if P is such that $\exists\, Q$ with $\underset{\displaystyle F}{\underset{\parallel}{P \oplus Q}}$ free, P is projective.

Proof. Exercise. Use the maps $P \overset{i}{\hookrightarrow} F$ and $F \twoheadrightarrow P$ along with projectivity of F. ∎

Remark. ① If $R \neq 0$ is a commutative ring and $R^n \overset{\text{as } R\text{-modules}}{\cong} R^m$, then $n = m$.

② $\exists$ a non comm. ring R s.t. $R \cong R^2$ as R-modules. Consequently $R^n \cong R^m$ $\forall\, n, m \in \mathbb{N}$.

EXAMPLE. Note $\mathbb{Z}/6 \cong \mathbb{Z}/2 \oplus \mathbb{Z}/3$.

Thus, $\mathbb{Z}/2$ and $\mathbb{Z}/3$ are projective $\mathbb{Z}/6$-modules.
However, neither is free.

Prop^n. Let k be a field, R a ring.
Suppose $k \subseteq Z(R)$ with $\dim_k(R) < \infty$.
Then, $R^n \cong R^m \Rightarrow n = m$.

Proof. $R^n \cong R^m$ as R-mod $\Rightarrow R^n \cong R^m$ as k-mod
$\Rightarrow n \cdot \dim_k R = m \cdot \dim_k R \Rightarrow n = m$. ∎

Remark. If $\alpha : M \to P$ is surjective with P projective, then
$\exists \sigma : P \to M$ s.t. $\alpha \circ \sigma = id_P$.
Thus, $M \cong P \oplus \ker \alpha$.

$$\begin{tikzcd} & P \arrow[dl, dashed, "\sigma"'] \arrow[d, equal, "id"] & \\ M \arrow[r, "\alpha"'] & P \arrow[r] & 0 \end{tikzcd}$$

In particular, if P is f.g., one can find a f.g. Q
s.t. $P \oplus Q \cong R^n$ with $n < \infty$.
(Map an R^n onto P and note Q is a quotient of R^n.)

Def^n. We say that the s.e.s. $0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} L \to 0$ splits
if $\exists \sigma : L \to N$ s.t. $\beta \circ \sigma = id_L$.

Remark. ① In the above case, we have $N \cong M \oplus L$.
② The above is equivalent to: $\exists \pi : N \to M$ s.t. $\pi \circ \alpha = id_M$.

Thm. Let R be a semisimple ring.
Then, every R-module is projective.

Proof. Let M be any R-module.
We get a s.e.s. $0 \to K \hookrightarrow F \to M \to 0$ with F free.
$K \subseteq F$. We have $F = K \oplus L$ as F is semisimple.
Thus, the above s.e.s. splits. Thus, $F \cong M \oplus K$ and hence,
M is projective. ∎

Lemma. $N \leq \mathbb{Z}^s \Rightarrow N \cong \mathbb{Z}^r$ for some $r \leq s$.

Submodule of a f.g. free module is free with rank not increasing.

Proof. Induction on s.

$s=1$: Clear since ideals are 0 or $n\mathbb{Z} \cong \mathbb{Z}$ for $n \neq 0$.

$s \geq 2$: $N \leq \mathbb{Z}^s = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_s$.

Let π_i denote the natural proj. $\mathbb{Z}^s \to \mathbb{Z}e_i$ and $j : N \hookrightarrow \mathbb{Z}^s$ the nat. inclusion.

CASE 1. $\pi_i \circ j = 0$ for some i.

Then, $N \leq \mathbb{Z}^{s-1}$ and by induction...

CASE 2. $\pi_i \circ j \neq 0$ for all i.

Then, $\operatorname{im}(\pi_i \circ j) = n_i \mathbb{Z}$ for all i, $n_i \geq 1$.

We have the s.e.s.

$$0 \to \ker(\pi_i \circ j) \longrightarrow N \xrightarrow{\pi_i \circ j / n} \mathbb{Z} \longrightarrow 0.$$

As $\mathbb{Z}$ is projective, we get

$$N \cong \mathbb{Z} \oplus \ker(\pi_i \circ j) \ldots$$

$\boxed{?}$

Lecture 8 (04-02-2022)

04 February 2022 17:26

Two classes of rings:

1. Noetherian rings: Hilbert Basis Theorem. → R commutative ⇓ R[x] commutative ⇓ $R[x_1, \dots, x_n]$ is comm.
2. Quiver algebras

Theorem. Let R be a left (resp. right) Noetherian ring. Then, R[x] is left (resp. right) Noetherian.

Proof. Let $I \subseteq R[x]$ be a left ideal. We wish to show that I is f.g. Can assume $I \neq 0$.

Notation: For $f = a_0 + a_1 x + \cdots + a_n x^n$ with $a_n \neq 0$, define $LT(f) := x^n$, $LC(f) := a_n$.

For $n \geq 1$, define

$$J_n := R\langle LC(f) : 0 \neq f \in I, \ LT(f) = x^n \rangle.$$

↳ left ideal generated in R by leading coeffs of n^{th} deg poly.s in I.

Note: J_n could be zero if no such f.

If $f = a_0 + \cdots + a_n x^n \in I$ with $a_n \neq 0$, then

$$LT(x f) = LT(f \cdot x) = x^{n+1}, \quad LC(x f) = a_n.$$

$\therefore J_n \subseteq J_{n+1}$.

We have an asc. chain of left ideals of R:

$$J_1 \subseteq J_2 \subseteq J_3 \subseteq \cdots.$$

As R is left Noe., the above stabilises. Let n_0 be s.t. $J_n = J_{n_0}$ $\forall n \geq n_0$.

$$J_{n_0} = (a_1, \dots, a_s).$$

Let $M = (R \oplus Rx \oplus \cdots \oplus Rx^{n_0 - 1}) \cap I.$

↓ Noetherian since R is.

M is a Noetherian R-module.
Write $M = R\langle m_1, \dots, m_r\rangle$.

Pick $f_1, \dots, f_s \in I$ of degree n_0 with $LT(f_i) = a_i$.

Claim: $I = R\langle m_1, \dots, m_r, f_1, \dots, f_s\rangle$.

Pf Let $N = R\langle m_1, \dots, m_r, f_1, \dots, f_s\rangle$.
Clearly, $N \subseteq I$.
Let $0 \neq f \in I$. We show $f \in N$ by induction on $\deg(f) =: n$.
If $n \leq n_0 - 1$, then $f \in M \subseteq N$.
Suppose $n \geq n_0$.
Then, $LC(f) \in J_n = J_{n_0}$.
Can subtract off leading term and decrease deg. ∎

Thus, we are done. ∎

Differential Rings

Let R be any ring.
$\delta : R \to R$ is a derivation if

$$\delta(a+b) = \delta(a) + \delta(b),$$
$$\delta(ab) = \delta(a)b + a\delta(b).$$

EXAMPLE. ① $R = k[x]$.
δ is $\frac{d}{dx}$.

② $R = k[x, y]$.
$\delta = x\frac{\partial}{\partial y}$.

$$R[x, \delta] := \left\{ \sum^{\infty} a_n x^n : a_n \in R,\ a_n = 0 \text{ for } n \gg 0 \right\}.$$

$$R[x, \delta] := \left\{ \sum_{n=0}^{\infty} a_n x^n \ : \ a_n \in R, \ a_n = 0 \text{ for } n \gg 0 \right\}.$$

Addition is usual.

Multiplication: $x \cdot a = ax + \delta(a)$.

Example ① $R = k[y, z]$, $\delta = \frac{\partial}{\partial y}$.

$S = R[x, \delta]$.

Let $a = y^2 + 2yz \in S$.

Then, $x \cdot a = a \cdot x + \delta(a)$

$= y^2 x + 2yzx + 2y + 2z.$

② Same as above but $\delta = \frac{\partial}{\partial z}$.

$x \cdot a = y^2 x + 2yzx + 2y.$

Theorem: Let R be left Noetherian, and $\delta : R \to R$ a derivation. Then, $R[x, \delta]$ is left Noetherian.
("right" as well.)

Proof. $S := R[x, \delta]$. Let $0 \neq I \subseteq S$ be a left ideal.
x need not be in the center anymore. $(x \in Z(S) \Leftrightarrow \delta \equiv 0.)$
Let $f = a_0 + a_1 x + \cdots + a_n x^n \in I$, $a_n \neq 0$.
Then, $x \cdot f = a_0 x + \delta(a_0) + a_1 x^2 + \delta(a_1) x + \cdots + a_n x^{n+1} + \delta(a_n) x^n$.
Then, $LC(xf) = a_{n+1}$.
Thus, the same proof as earlier goes through. ☐

Lecture 10 (11-02-2022)

11 February 2022 17:34

Krull Schmidt Theorem

Def^n. Let $R \neq 0$ be a ring. Let $E \neq 0$ be an R-module. E is said to be decomposable if $E = E_1 \oplus E_2$ for some nonzero submodules E_1, E_2.

E is said to be indecomposable if it is not decomposable.

- Ring structure on $\mathrm{Hom}_R(E, E) = \mathrm{End}_R(E)$ is given by pointwise $+$ and composition $(f \cdot g := f \circ g)$ as the multiplication.

If $E \neq 0$, then $\mathrm{Hom}_R(E, E) \neq 0$ as 0 and id_E are distinct endomorphisms.

Def. A ring $S \neq 0$ is said to be local if the set of nonunits is a two-sided ideal.

Lemma 1 $\underset{(\Downarrow \; E \neq 0)}{\mathrm{End}_R(E) \text{ is local}} \Rightarrow E$ is indecomposable.

Proof. Suppose not. Write $E = E_1 \oplus E_2$ for $E_1, E_2 \neq 0$.

We have the projection maps $\pi_1, \pi_2 \in \mathrm{End}_R(E)$.

π_1, π_2 are not onto. Thus, π_1, π_2 are nonunits.

Thus, $\underbrace{\pi_1 + \pi_2}_{= \mathrm{id}_E}$ is a nonunit. $\rightarrow \leftarrow$ $\blacksquare$

EXAMPLE. Converse not true. $\mathbb{Z}$ is indecomposable but $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}) \cong \mathbb{Z}$ is NOT local.

Lemma 2 Let $E \overset{\neq 0}{}$ be a finite length module (Noetherian + Artinian).

E indecomposable $\Rightarrow \mathrm{End}_R(E)$ is local.

Before that, we prove something else:

Setup

Let $E \neq 0$ be a finite length module (possibly decomposable).
(Artinian + Noetherian)

By assumption, $(\ker(u^n))_{n\geq 1}$ and $(\mathrm{im}(u^n))_{n\geq 1}$ stabilise, say to $\ker(u^\infty)$ and $\mathrm{im}(u^\infty)$, respectively.

Lemma 3. (Fitting Lemma) With the above notation we have:

(1) $E = \mathrm{im}(u^\infty) \oplus \ker(u^\infty)$.

(2) $u(\ker u^\infty) \subseteq \ker u^\infty$. $u|_{\ker u^\infty}$ is nilpotent.

(3) $u(\mathrm{im}\ u^\infty) \subseteq \mathrm{im}\ u^\infty$. $u|_{\mathrm{im}\ u^\infty}$ is an isomorphism.

Proof. Let $N \gg 0$ be s.t. $\ker u^N = \ker u^\infty$ and $\mathrm{im}\ u^\infty = \mathrm{im}\ u^N$.

(1) Claim (i) $\ker u^\infty \cap \mathrm{im}\ u^\infty = 0$.

Proof. Let $x \in \ker u^\infty \cap \mathrm{im}\ u^\infty$.

$x = u^N(y)$. Also, $0 = u^N(x) = u^{2N}(y)$.

$\therefore\ y \in \ker u^{2N} = \ker u^N$. $\therefore\ x = u^N(y) = 0$. ∎

Claim (ii) $\mathrm{im}\ u^\infty + \ker u^\infty = E$.

Proof. Let $x \in E$.

$u^N(x) \in \mathrm{im}\ u^N = \mathrm{im}\ u^{2N}$. $\therefore\ u^N(x) = u^{2N}(y)$ for some $y \in E$.

Now, $x = \underset{\mathrm{im}\ u^N}{\underset{\cap}{u^N(y)}} + \underset{\ker u^N}{\underset{\cap}{(x - u^N(y))}}$. ∎

Thus, $E = \ker u^\infty \oplus \mathrm{im}\ u^\infty$.

(2) $u(\ker u^\infty) \subseteq \ker u^\infty$ is clear.

Indeed, if $x \in \ker u^\infty = \ker u^N$, then $u^N(ux) = 0$.

Thus, u is an endomorphism of $\ker u^\infty$.

Clear that $(u|_{\ker u^\infty})^N = 0$.

Check that $(u|_{\ker u^\infty})^N = 0$.

If $x \in \ker u^\infty$, then $x \in \ker u^N$. Thus, $u^N(x) = 0$. ∎

(3) Check $u(\operatorname{im} u^\infty) \subseteq \operatorname{im} u^\infty$.

Let $\alpha = u|_{\operatorname{im} u^\infty} \in \operatorname{End}_R(\operatorname{im} u^\infty)$.

As $\operatorname{im} u^\infty$ is Artinian, it suffices to show that α is injective.

It follows that α is an iso.

But $\ker(\alpha) = 0$ follows essentially by proof of Claim (i). ∎

Now, we prove Lemma 2 : E indec + finite length $\Rightarrow \operatorname{End}_R(E)$ is local.

Proof. Let $S = \operatorname{End}_R(E) \neq 0$ (as $E \neq 0$).

Let $J = \{u : E \to E \mid u$ is a nonunit$\}$.

Let $u \in J$ be arbitrary.

Fitting : $E = \operatorname{im} u^\infty \oplus \ker u^\infty$.

Indecom : $E = \operatorname{im} u^\infty$ or $\ker u^\infty$.

But $u|_{\operatorname{im} u^\infty}$ is iso. $\therefore \operatorname{im} u^\infty = 0$.

Thus, $\ker u^\infty = E$ and every $u \in J$ is nilpotent.

Conversely, any nilpotent is in J.

To show: that J is an ideal.

As E is finite length, we see that nonunit $\Leftrightarrow$ not 1-1

$\Leftrightarrow$ not onto.

Let $u \in J$, $v \in S$. Then, $u \circ v$ is not onto and

$v \circ u$ is not 1-1.

Lastly, let $u, v \in J$. TS : $u + v \in J$.

Suppose $u + v$ is invertible.

Let $\xi_1 = u \circ (u+v)^{-1}$, $\xi_2 = v \circ (u+v)^{-1}$.

Then, $\xi_1, \xi_2 \in J$ by earlier and $\xi_1 + \xi_2 = 1$.

Note $\xi_1 = 1 - \xi_2$ is invertible $((1-\xi_2)^{-1} = 1 + \xi_2 + \xi_2^2 + \dots)$.

This is a contradiction. ∎

Lecture (04-03-2022)

04 March 2022 17:31

Radical of a Ring

Let $R \neq 0$. An application of Zorn's lemma tells us that there exists a maximal left (resp. right) ideal in R.

Def^n. The left radical of a ring $R \neq 0$ is defined as

$$^{\ell}\mathrm{rad}(R) = \bigcap_{\mathfrak{m}\,:\,\text{left max'l}} \mathfrak{m}.$$

Similarly, one defines the right radical ideal $^{r}\mathrm{rad}(R)$.
We will show $^{\ell}\mathrm{rad}(R) = {}^{r}\mathrm{rad}(R)$ and define $\mathrm{rad}(R)$ to be this common ideal. In particular, it is a two-sided ideal.

Examples. $R = k[x_1, \dots, x_n]$. $\quad \mathrm{rad}(R) = 0$.

$\mathfrak{m} = (x_1, \dots, x_n)$.

$\mathrm{rad}(R_{\mathfrak{m}}) = \mathfrak{m}R_{\mathfrak{m}} \neq 0$.

In general, if $(R, \mathfrak{m})$ is a local comm. ring, then $\mathrm{rad}(R) = \mathfrak{m}$.

For the time being, define $\mathrm{rad}(R) := {}^{\ell}\mathrm{rad}(R)$ for ease of convenience.

Lemma. Let $R \neq 0$ and $y \in R$.
TFAE:

(i) $y \in \mathrm{rad}(R)$,

(ii) $1 - xy$ is left invertible for all $x \in R$,

(iii) $yM = 0$ for all simple left R-modules M.

Proof. (i) $\Rightarrow$ (ii). $\quad y \in \mathrm{rad}(R) \Rightarrow y \in L \;\; \forall$ left max'l L

$$\Downarrow$$

$1 - xy \notin L \;\; \forall L \;\; \forall x \;\Leftarrow\; xy \in L \;\; \forall L \;\; \forall x$

$$\Downarrow$$

$1-xy$ is left invertible $\forall x$.

(ii) $\Rightarrow$ (iii) Let M be a simple R-module.

If $yM \neq 0$, then $\exists p \in M$ s.t. $yp \neq 0$. (In particular, $p \neq 0$.)

By simplicity, $Ryp = M$.

$\therefore \exists x \in R$ s.t. $xyp = p$ or $(1-xy)p = 0$.

But then $p = 0$. $\rightarrow\leftarrow$

(iii) $\Rightarrow$ (i) Let L be a max'l left ideal.

Then, R/L is a simple left R-mod.

Thus, $y(R/L) = 0$ or $y \in L$. ∎

We now show that $\mathrm{rad}(R)$ is a two-sided ideal.

Given a left R-module M, define

$$\mathrm{ann}_R(M) := \{a \in R : aM = 0\}.$$

$\mathrm{ann}_R(M)$ is a two-sided ideal of R.

Suppose $y \in \mathrm{rad}(R)$. Then, $y \in \bigcap_{L \text{ max'l left}} \mathrm{ann}_R(R/L)$. any simple module is of this form

OTOH, each $\mathrm{ann}_R(R/L)$ is the intersection $\bigcap_{\substack{\bar{x} \neq 0 \\ \bar{x} \in R/L}} \mathrm{ann}_R(\bar{x})$ of left ideals.

Thus, $$\mathrm{rad}(R) = \bigcap_{L \text{ left max'l}} \mathrm{ann}_R(R/L).$$

Thus, $\mathrm{rad}(R)$ is a two-sided ideal.

Lemma. For $y \in R^{\neq 0}$, TFAE:

(i) $y \in \mathrm{rad}(R)$,

(ii) $1 - xyz$ is a unit for all $x, z \in R$.

Corollary. ${}^{\ell}\mathrm{rad}(R) = {}^{r}\mathrm{rad}(R)$. ($\because$ (ii) is symmetric.)

Proof. (ii) $\Rightarrow$ (i) is clear. Take $z = 1$ and use earlier result.

(i) $\Rightarrow$ (ii). $\quad y \in \mathrm{rad}(R) \Rightarrow yz \in \mathrm{rad}(R)$ since two-sided ideal.

$\therefore \exists u \in R$ s.t. $u(1 - xyz) = 1$.

$\Rightarrow \quad u = 1 + \underbrace{uxyz}_{\in \mathrm{rad}(R)}$

Thus, u has a left inverse. It already has a right inverse. Thus, u is a unit and hence, so is $1-xyz$. ☐

Proposition. Let $J \trianglelefteq R$ be an ideal s.t. $J \subseteq \mathrm{rad}(R)$. ($J \neq 0$)

Then, $\mathrm{rad}(R/J) = \dfrac{\mathrm{rad}(R)}{J}$.

(Exercise)

AP. : Find an example s.t. $J \nsubseteq \mathrm{rad}(R)$ and $\mathrm{rad}(R/J) \neq \dfrac{\mathrm{rad}(R)+J}{J}$.

Prop^n. R and $R/\mathrm{rad}(R)$ have same simple left R-modules.

In other words, every simple left R-module is annihilated by $\mathrm{rad}(R)$.

But we saw that $\mathrm{rad}(R)$ is the intersection of ann of all simple R-modules.

Lemma (Nakayama Lemma)

Let M be a f.g. left R-module and $M = JM$.

Then, $M = 0$.

Proof. Suppose $JM = M$ and $M \neq 0$.

Write $M = \langle m_1, \ldots, m_s \rangle$ with $s \geq 1$ minimal.

$$m_s = a_1 m_1 + \cdots + a_s m_s \quad \text{for some } a_i \in J \text{ since } M = JM.$$

$$\Rightarrow (1-a_s) m_s = a_1 m_1 + \cdots + a_{s-1} m_{s-1}.$$

But $1-a_s$ is a unit. This contradicts minimality of s. ☐

Def^n. Let I, J be left ideals.

IJ is the left ideal generated by $\{ij : i \in I, j \in J\}$.

$T^n = T \cdot \cdots \cdot T$

all finite sums of this form

I is nil if $\forall a \in I : \exists n \in \mathbb{N}$ s.t. $a^n = 0$.
I is nilpotent if $I^n = 0$ for some n.

Remark. (1) I nilpotent $\Rightarrow$ I nil.
(2) ($\not\Leftarrow$) $R = k[x_1, \dots, x_n, \dots] / (x_1, x_2^2, \dots, x_n^n, \dots)$.
Let $\eta = (\bar{x}_1, \bar{x}_2, \bar{x}_3, \dots)$.
Then, η is nil but not nilpotent.
since R is comm and each generator is nilpotent

For comm Noe : nil $\Leftrightarrow$ nilpotent.
In general : R comm, I f.g : I nil $\Leftrightarrow$ I nilpotent.

Lemma. I left nil ideal in R $\Rightarrow$ $I \subseteq \operatorname{rad}(R)$.

Proof. Let $y \in I$ and $x \in R$ be arbitrary.
Then, $xy \in I$ and hence is nilpotent.
Thus, $1 - xy$ is invertible (take $1 + xy + (xy)^2 + \cdots$) and we are done. ☒

Lecture (08-03-2022)

08 March 2022 17:21

Recap Last time, we looked at rad(R) − radical of R.

$$\mathrm{rad}(R) \overset{\text{def}}{=} \bigcap_{\substack{\mathfrak{m}:\text{ max'l}\\ \text{left ideal}}} \mathfrak{m} \overset{\text{theorem}}{=} \bigcap_{\substack{\mathfrak{m}:\text{ max'l}\\ \text{left}}} \mathrm{ann}_R(R/\mathfrak{m}) \overset{\text{theorem}}{=} \bigcap_{\mathfrak{y}:\text{ max'l right}} \mathfrak{y}.$$

$\therefore$ rad(R) is a two-sided ideal of R

- $y \in \mathrm{rad}(R) \iff 1-xy$ is left invertible $\forall x \in R$
  $\iff yM = 0$ for every simple left R-module M.
  $\iff 1 - xyz$ is invertible $\forall x, z \in R$
  $\iff 1 - yz$ is right invertible $\forall z \in R$

- M is a simple left R-mod $\Rightarrow$ $\mathrm{rad}(R) \subseteq \mathrm{ann}_R(M)$.
  $\therefore$ R and $R/\mathrm{rad}(R)$ have the same simple left modules.

- M f.g. left R-module, $J \subseteq \mathrm{rad}(R)$. $JM = M \Rightarrow M = 0$. } Nakayama lemma

- I : left ideal. I is nil iff $\forall a \in I, \exists n \in \mathbb{N}$ s.t. $a^n = 0$.
  I is nilpotent iff $\exists n \in I$ s.t. $I^n = 0$.
  I nil $\Rightarrow I \subseteq \mathrm{rad}(R)$.

Lemma. Let $R^{\neq 0}$ be a left Artinian ring. Then
(i) A nil ideal is nilpotent.
(ii) rad(R) is nilpotent.

Proof. Suffices to prove (ii) since any nil ideal is contained in rad(R).
Let $J = \mathrm{rad}(R)$. Then, we have

$$J \supseteq J^2 \supseteq J^3 \supseteq \cdots$$

By Artin hypothesis, $J^n = J^{n+1}$ for some n.

We now show that $J^n = 0$ and finish the proof.

Suppose, if possible, $J^n \neq 0$. Let $I = J^n$.

Let
$$\mathcal{C} = \{ q : q \text{ is a left ideal and } Iq \neq 0 \}.$$
$\mathcal{C} \neq \emptyset$ since $J \in \mathcal{C}$.

Pick $L \in \mathcal{C}$ min'l (note that R is left Artin).

$I \neq 0$. Pick $a \in L$ s.t. $Ia \neq 0$.

Then, $I(Ra) \neq 0$. By min'l, $Ra = L$.

$IJL = IJL = IL \neq 0$.

By min'l, $JL = L$. But L is f.g.

By NAK, $L = 0$.

But $IL \neq 0$. $\rightarrow\leftarrow$ ∎

Theorem. Let $R \neq 0$ be a ring. TFAE:

(i) R is semisimple.

(ii) R is left Artin and $\text{rad}(R) = 0$.

(iii) R is right Artin and $\text{rad}(R) = 0$.

(i) is symmetric in "left" and "right" and so is $\text{rad}(R)$.

$\therefore$ suffices to show (i) $\Leftrightarrow$ (ii).

Proof. (i) $\Rightarrow$ (ii) By Wedderburn Artin,
$$R \cong \prod_{i=1}^{s} M_{n_i}(D_i). \quad \therefore R \text{ is left Artin.}$$

As R is semisimple, we can write $R = \text{rad}(R) \oplus L$.

Thus, $\text{rad}(R) \cong R/L$ is f.g.

By earlier, $(\text{rad}(R))^n = 0$ for some $n \geq 1$.

By NAK ($\because \text{rad}(R)$ is f.g.), $\text{rad}(R) = 0$.

(ii) $\Rightarrow$ (i) $R^{\neq 0}$: left Artin and $\text{rad}(R) = 0$.

Let I be a min'l nonzero left ideal.

Then, I is a simple R-module.

$\because \text{rad}(R) = 0$, $\exists\, \mathfrak{m}$ max'l left ideal s.t. $I \not\subseteq \mathfrak{m}$.

$\left(\because I \neq 0 \text{ and } \text{rad}(R) = \bigcap_{\mathfrak{m}:\text{ max'l left}} \mathfrak{m} = 0. \right)$

$\therefore R = I \oplus \mathfrak{m}$. $\left(\mathfrak{m} \text{ max'l} \Rightarrow I + \mathfrak{m} = R. \right)$

left

$\therefore R = I \oplus \mathfrak{m}$. ($\mathfrak{m}$ max'l $\Rightarrow I + \mathfrak{m} = R$. I simple & $I \notin \mathfrak{m} \Rightarrow I \cap \mathfrak{m} = 0$.)

Put $I_1 = I$.

Now, if $\mathfrak{m} \neq 0$, then continue similarly by picking $0 \neq I_2 \subseteq \mathfrak{m}$ min'l. By Artin, this stops and we get

$$R = I_1 \oplus I_2 \oplus \cdots \oplus I_n \text{ for simple left ideals } I_i. \qquad \square$$

Theorem (Converse of Maschke)

Let k be a field and G a finite group. Suppose $\operatorname{char}(k) \mid |G|$. Then, $k[G]$ is not semisimple.

Proof. Let $n = |G|$. Put $s = \sum_{g \in G} g$.

Note $hs = s = sh$ for all $h \in G$.
Thus, ks is a two-sided ideal of $k[G]$.

But

$$s^2 = \sum_{g \in G} gs = \sum_{g \in G} s = |G| s = 0.$$

Thus, ks is a nilpotent nonzero ideal. $\therefore \operatorname{rad}(k[G]) \neq 0$.
$\therefore k[G]$ is not semisimple. $\square$

Hopkin – Levitski Theorem

Lemma 1. $R^{\neq 0}$: left Artin $\Rightarrow R/\operatorname{rad}(R)$ is semisimple.

Proof. $\operatorname{rad}\left(R/\operatorname{rad}(R)\right) = \operatorname{rad}(R)/\operatorname{rad}(R) = 0$.

Also, $R/\operatorname{rad}(R)$ is left Artin. $\square$

Lemma 2. A finite direct sum of (left) simple modules is both Artinian and Noetherian.

Lemma 3. Let S be a semisimple ring. M is a left S-module.
TFAE:

(i) M is Artinian.

(ii) M is Noetherian.

Proof. $M = \bigoplus_{\alpha \in \Lambda} M_\alpha$, with Λ possibly infinite, M_α simple.

Note that an Artinian (resp. Noetherian) module cannot contain an infinite direct sum of non zero modules.

$\left(\text{Consider} \quad M_1 \subsetneq M_1 \oplus M_2 \subsetneq M_1 \oplus M_2 \oplus M_3 \subsetneq \cdots \quad \text{or} \quad \bigoplus_{i=1}^{\infty} M_i \supsetneq \bigoplus_{i=2}^{\infty} M_i \supsetneq \bigoplus_{i=3}^{\infty} M_i \supsetneq \cdots \right)$

Thus, (i) $\iff |\Lambda| < \infty \iff$ (ii). $\blacksquare$

Theorem. R left Artinian $\Rightarrow$ R left Noetherian.

Proof. Can assume $R \neq 0$.

Let $J = \text{rad}(R)$. Pick $n \geq 1$ s.t. $J^n = 0$. $(J^0 := R.)$

R/J is semisimple. J^i Artin R-module.

J^i / J^{i+1} is an Artin R/J-module.

$\therefore J^i / J^{i+1}$ is a Noe. R/J-module.

$\therefore J^i / J^{i+1}$ is a Noe. R-module.

For $i = n-1$, we get J^{n-1} is a Noe. R-module.

Consider the s.e.s.

$$0 \to J^{i+1} \to J^i \to J^i / J^{i+1} \to 0.$$

By backward induction we get $J^{n-1}, J^{n-2}, \ldots, J, R$ are all Noe! $\blacksquare$

Lecture (15-03-2022)

15 March 2022 17:31

Let $R \neq 0$ be a ring.
We say that R can be ordered if there exists a total order '$<$' on R s.t.

$$a < c \Rightarrow a+b < c+b,$$

$$a > 0,\ b > 0 \Rightarrow ab > 0.$$

EXAMPLES. (i) $\mathbb{Z}$, $\mathbb{R}$ usual order.
(ii) $\mathbb{C}$ not ordered. In general, $a^2 > 0$ $\forall a \neq 0$ in an ordered ring and $-1 < 0$.

Let $R \neq 0$ be an ordered ring.
Set $P = \{a \in R : a > 0\}$.
Then,
(i) $P + P \subseteq P$,
(ii) $P \cdot P \subseteq P$,
(iii) $P \cup -P = R \setminus \{0\}$.

Conversely, if $P \subseteq R$ satisfies (i) $-$(iii), then we can define an order on R by $a > b \Leftrightarrow a - b \in P$.
P is called an ordering on R.

Prop^n. Let $P \subseteq R$ be an ordering on R. Then,
(i) $P \cap -P = \emptyset$,
(ii) $1 \in P$,
(iii) $\mathrm{char}(R) = 0$,
(iv) R is a domain.

$a \in P \cap (-P) \Rightarrow a, -a \in P$
$\Rightarrow \pm a^2 \in P$
$\Rightarrow 0 \in P \rightarrow \leftarrow$
$P \cap \{\pm 1\} \neq \emptyset$. $\therefore 1 = (-1)^2 = 1^2 \in P$.

Proof. Exercise.

Pre-ordering on a ring R.

Def^n. A preordering in a ring $R^{\neq 0}$ is a subset $T \subseteq R\setminus\{0\}$ s.t.

(1) $T + T \in T$,

(2) for $a_1, \ldots, a_m \in R\setminus\{0\}$ and $t_1, \ldots, t_n \in T$,
then product of $\underbrace{a_1, a_1, \ldots, a_m, a_m}_{\text{all must appear twice}}, t_1, \ldots, t_n$ in any order is in T.

- R need not be commutative.

Let F be a field of char $= 0$.
Set
$$T_0(F) = \{ x \in F : x \text{ is a (nonempty!) finite sum of (nonzero!) squares} \}.$$

If $0 \notin T_0(F)$, then $T_0(F)$ is a pre-order & $T_0(F) \subseteq T$ $\forall$ pre-ordering T on F.

Exercise Let $T \subseteq R$ be a preordering.

(i) $T \cap (-T) = \emptyset$,

(ii) $1 \in T$,

(iii) char $(R) = 0$,

(iv) R is a domain.

Theorem. (Proof Later)

Let $R^{\neq 0}$ be a ring s.t.
$$\mathcal{C} = \{ T \subset R : T \text{ is a preordering} \}.$$
Order $\mathcal{C}$ by inclusion. Suppose $\mathcal{C} \neq \emptyset$.

(i) $\mathcal{C}$ satisfies the hypothesis of Zorn's lemma.

(ii) Any maximal element of $\mathcal{C}$ is an ordering.

Theorem. (Artin-Schrier)

Let F be a field with char$(F) = 0$.
Suppose $-1 \notin T_0(F)$.
Then, F is orderable. (F orderable $\Rightarrow$ $-1 \notin T_0(F)$ is clear.)

Proof. Only need to check that $0 \notin T_0(F)$. Then, $\mathcal{C}$ as in prev. thm is nonempty since $T_0(F)$ is a preordering then.

$$0 = \sum_{i=1}^{n} a_i^2 \qquad (n \geq 1 \text{ and } a_1 \neq 0 \text{ can be assumed.})$$

$$\Rightarrow a_1^2 = -\sum_{i=2}^{n} a_i^2$$

$$\Rightarrow 1 = -\sum \left(\frac{a_i}{a_n}\right)^2.$$

$\blacksquare$

Artin-Schreier proved that:

If $F \subseteq K$ and K is alg. closed with $1 < \dim_F K < \infty$,

then (1) $\mathrm{char}(F) = 0$,

(2) $\dim_F(K) = 2$,

(3) $K = F(\sqrt{-1})$,

(4) F is formally real in our sense (orderable).

F is called a real closed field in this case.

Lecture (22-03-2022)

22 March 2022 17:26

Always assume $R \neq 0$.

Recall: R is said to be an ordered ring if there is a total order $<$ s.t.

(i) $a < b \Rightarrow a + c < b + c$,

(ii) $a, b > 0 \Rightarrow ab > 0$.

$\mathbb{Z}, \mathbb{Q}, \mathbb{R} \longrightarrow$ ordered

$\mathbb{C} \longrightarrow$ cannot be ordered

Theorem. (Artin-Schreier.)

Let F be a field of char $= 0$.

TFAE:

(i) F can be ordered.

(ii) -1 is not a finite sum of squares.

- An ordering of R is a subset $P \subset R$ s.t.
  - (i) $P + P \subseteq P$,
  - (ii) $P \cdot P \subseteq P$,
  - (iii) $P \cup -P = R \setminus \{0\}$.

- $< \longleftrightarrow P$

$a < b \Leftrightarrow b - a \in P$; $P := \{a : a > 0\}$.

Prop^n. Suppose $P \subseteq R$ is an ordering. Then,

(i) $P \cap (-P) = \phi$,

(ii) $1 \in P$,

(iii) char $R = 0$,

(iv) R is a domain.

- $T \subseteq R\setminus\{0\}$ is called a preorder if
  (i) $T + T \subseteq T$,
  (ii) if $a_1, \dots, a_n \in R\setminus\{0\}$ and $t_1, \dots, t_m \in T$, $(n, m \geq 0)$
  then the product of $a_1, a_1, \dots, a_n, a_n, t_1, \dots, t_m$
  in any permutation belongs to T.

  (For commutative R: $a_1^2 \cdots a_n^2 \, t_1 \cdots t_m \in T$.
  Non comm: $a_1^2 t_1$, $a_1 t_1 a_1$, $a_1^2 t_2 t_1 a_2 t_3 a_2, \dots \in T$.)

Ex. $R \neq 0$. $T \subseteq R\setminus\{0\}$ be a preordering. Then,
(i) $T \cap (-T) = \emptyset$,
(ii) $1 \in T$,
(iii) $\mathrm{char}(R) = 0$,
(iv) R is a domain.

Theorem Let $R^{\neq 0}$ be a ring.
Define
$$\mathcal{C} := \{ T \subset R : T \text{ is a pre-ordering}\}.$$
Assume $\mathcal{C} \neq \emptyset$. Partial ordering $\mathcal{C}$ w.r.t. $\subseteq$.
(i) $\mathcal{C}$ satisfies the hypothesis of Zorn's lemma.
(ii) Maximal elements of $\mathcal{C}$ are orderings on R.

From the above, Artin-Schreir follows since
$$T_0(F) = \{\text{non empty finite sums of non zero squares}\}$$
does not contain 0 as $-1 \neq \sum$ squares. $T_0(F)$ is a preorder. ☒

Extending Preorderings

Let T be a preordering on R.
Let $b \in R\setminus\{0\}$.

$$B(T)_b = \left\{ x \in R : \begin{array}{l} x \text{ is a product of a permutation of} \\ b^i, a_1, a_1, \ldots, a_m, a_m, t_1, \ldots, t_n \\ \text{for } i \geq 0, \ m \geq 0, n \geq 0, \\ a_j \in R \setminus \{0\}, \quad t_j \in T \end{array} \right\}.$$

Let T_b = non empty finite sums of elements in $B(T)_b$. (Not squares!)

Check:
1) $T_b + T_b \subseteq T_b$.
2) $T \subseteq T_b$.
3) Any permutation of
$a_1', a_1', \ldots, a_m', a_m', t_1', \ldots, t_n'$
is in T_b. As usual $a_j' \in R\setminus\{0\}$ and $t_j' \in T_b$.

Remark: T_b is a preordering $\iff 0 \notin T_b$.

Lemma A. Let $R \neq 0$ be a ring. TFAE:
(i) T_b is not a preordering on R.
(ii) $\exists\, t, t' \in T$ s.t. $t' + bt = 0$.
(iii) $\exists\, t, t' \in T$ s.t. $t' + tb = 0$.

Proof (ii) $\Rightarrow$ (iii): $t' + bt = 0$

$$\Rightarrow t'b + \underbrace{btb}_{\in T,} = 0.$$

$\in T$, since T is a preorder and $b \neq 0$

(iii) $\Rightarrow$ (ii): similar.

(i) $\Rightarrow$ (ii): Suppose T_b is not a preordering.
$\therefore 0 \in T_b$.
$\Rightarrow 0 = x_1 + \cdots + x_\ell$,
where $\ell \geq 1$ and $x_i \in B(T)_b$.
$\therefore$ Each x_i is some permutation of ...
Depending on the power of b appearing in x_i,
we have $x_i \in T$ or $b x_i \in T$.

$$\Rightarrow \quad 0 = \underbrace{x_1 + \cdots + x_r}_{\in T} + \underbrace{x_{r+1} + \cdots + x_\ell}_{b \cdot x_k \in T}$$

$$\Rightarrow \quad 0 = \underbrace{b(x_1 + \cdots + x_r)}_{\in T} + \underbrace{b x_{r+1} + \cdots + b x_\ell}_{\in T}. \qquad ☒$$

Theorem B. Let $R^{\neq 0}$ be a ring.

Assume

$$\mathcal{C} := \{ T \subseteq R : T \text{ is a preordering} \} \neq \emptyset.$$

Then: (i) $\mathcal{C}$ satisfies the hypothesis of Zorn's lemma.

(ii) Let $T \in \mathcal{C}$. T is max'l $\Leftrightarrow$ T is an ordering on R.

Proof. (i) Let $\{T_\alpha\}_{\alpha\in\Lambda}$ be a chain in $\mathcal{C}$.

Set $\quad T := \bigcup_{\alpha\in\Lambda} T_\alpha$.

Claim: $T \in \mathcal{C}$. This would finish the proof.

Pf. Usual. All conditions involve finitely many elements.

Pick α large enough.

$0 \notin T$ since $0 \notin T_\alpha \ \forall \alpha$. ☒

(ii) Let T be an ordering on R.

Claim: T is maximal in $\mathcal{C}$.

Proof. Suppose not. Then, $\exists T' \in \mathcal{C}$ with $T \subsetneq T'$.

Pick $a \in T' \setminus T$. Then, $a \neq 0$.

Thus, $-a \in T \subseteq T'$.

But then $0 = a + (-a) \in T'$. $\rightarrow\leftarrow$

Conversely, now assume that $T \in \mathcal{C}$ is max'l.

Claim: T is an ordering.

Proof. Suppose not. Then, $T \cup (-T) \subsetneq R \setminus \{0\}$.

Pick $b \neq 0$ s.t. $\{b, -b\} \cap T = \emptyset$.

Now, $T \subsetneq T_b$.

$\therefore T_b \notin \mathcal{C}$ by max'l'ty of T.

That is, T_b is not a preordering.

$\therefore t_1 + bt_2 = 0$ for some $t_1, t_2 \in T$.

Similarly,

$t_3 - bt_4 = 0$ — " — $t_3, t_4 \in T$.

$t_1 = -bt_2, \quad t_3 = bt_4$.

$\therefore t_1 t_3 = -b^2 t_2 t_4$.

$$\therefore \underbrace{\underbrace{t_1 t_3}_{\in T} + \underbrace{b^2 t_2 t_4}_{\in T}}_{\in T} = 0.$$

$\therefore 0 \in T$. $\rightarrow\leftarrow$

This finishes the proof. ☒

Let $R^{\neq 0}$ be a ring. Let $T_0(R)$ be nonempty finite sums of $a_1, a_1, \ldots, a_n, a_n$. $a_i \in R \setminus \{0\}$.

Check: $T_0(R)$ is not a Preorder $\Leftrightarrow 0 \in T_0(R)$.

Def^n R is said to be formally real if $0 \notin T_0(R)$.

Theorem C. TFAE:

(i) R is formally real.

(ii) R has a preordering.

(iii) R has an ordering.

Proof. (iii) $\Rightarrow$ (ii) OK.

(ii) $\Rightarrow$ (iii) Theorem B.

(iii) $\Rightarrow$ (i): let T be an ordering on R

Then, $T_0(R) \subseteq T$. (Check.)

$\therefore\ 0 \notin T_0(R)$.

(i) $\Rightarrow$ (ii) : $T_0(R)$ is a preordering. $\blacksquare$

Lecture (25-03-2022)

25 March 2022 17:30

Example.

$\mathbb{Q}(t)$ = Field of fractions of $\mathbb{Q}[t]$.

leading coefficient

Whenever we write $\frac{f(t)}{g(t)} \in \mathbb{Q}(t)$, we assume $LC(g(t)) > 0$.

$$P = \left\{ \frac{f(t)}{g(t)} : LC(f(t)) > 0 \right\} \quad \text{defines an ordering.}$$

Note $t - n \in P \quad \forall n \in \mathbb{N}$.

$\therefore \quad t > n \quad \forall n \in \mathbb{N}$ (in this ordering).

Also, $\frac{1}{t} < \frac{1}{n} \quad \forall n \in \mathbb{N}$.

Def. Let $(R, <)$ be an ordered ring.

(i) $a \in R$ is infinitely big if

$a > n$ for all $n \in \mathbb{N}$.

(ii) $a \in R$ is infinitely small if

$a > 0$ and $na < 1$ for all $n \in \mathbb{N}$.

(iii) R is said to be Archimedean if

$\forall a, b \in R_{>0} \ \exists m \in \mathbb{N}$ s.t. $a < mb$.

Examples.

(1) $\mathbb{R}$ is Archimedean.

(2) $\mathbb{Q}(t)$ is not Archimedean. $t, 1 > 0$ but $m \cdot 1 < t \ \forall m$.

(3) Let $\mathbb{Q}[t]$ and $\mathbb{Q}[1/t]$ have the ordering induced from $\mathbb{Q}(t)$.

Then, $\mathbb{Q}[t]$ has inf. big elements but no inf. small element.

Reverse for $\mathbb{Q}[1/t]$.

Proposition. Let $(R, <)$ be an ordered ring. TFAE:

(1) R is Archimedean.

(2) R has no inf. large or small elements.

Proof. $(\Rightarrow)$ Let $x > 0$. As R is Arch, $\exists\, n^{\in \mathbb{N}}$ s.t. $x < 1 \cdot n$.

$\therefore x$ is not inf large.

llly $\exists\, m \in \mathbb{N}$ s.t. $1 < mx$.

$(\Leftarrow)$ Let $a, b > 0$ be given.

Pick $n, m \in \mathbb{N}$ s.t. $b < n$ and $ma > 1$.

Then, $mn\, a > n > b$. Thus, R is Archimedean. ∎

Theorem (Hilbert)

Let $(R, <)$ be an Archimedean ordered ring.

Then,

1) There is an injective ring homomorphism

$$i : R \longrightarrow \mathbb{R}$$

which preserves order, i.e., $a < b \Rightarrow i(a) < i(b) \quad \forall a, b \in R$.

2) The only order preserving ring homomorphism $\mathbb{R} \to \mathbb{R}$ is the identity.

We don't prove the result. Refer Lam.

Lemma. Let $(R, <)$ be an Archimedean ordered ring.

Then, R is commutative.

Proof. Let $a, b \in R$. TS: $ab = ba$.

Can assume $a, b > 0$.

Let $m \in \mathbb{N}$.

By Arch., $\exists\, n^{\in \mathbb{N}}$ s.t. $na > mb$.

Choose the smallest such n, call it n_0.

$$(n_0 - 1)a \le mb < n_0 a.$$

$$\begin{aligned} m(ba - ab) &= mba - mab \\ &< n_0 a^2 - (n_0 - 1)a^2 \\ &= a^2 \end{aligned}$$

$\Rightarrow \quad m(ba - ab) < a^2 \qquad \forall\, m \in \mathbb{N}.$

$= a^2$

$\Rightarrow \quad m(ba - ab) < a^2 \qquad \forall\, m \in \mathbb{N}.$

$\Rightarrow \quad ba - ab \leq 0$ (Use Arch on $ba-ab$ and a^2 else.)

$\Rightarrow \quad ba \leq ab.$

By symmetry, $ab \leq ba$.

$\therefore \quad ba \leq ab \leq ba.$ ∎

Division Rings.

Theorem. (Wedderburn's Little Theorem)

Let D be a finite division ring.
Then, D is a (commutative) field.

Proof. $Z(D) = F$ is a finite field.

$|F| = q = p^k.$ (p prime, $k \in \mathbb{N}$.)

Consider D as a vector space over F.

Let $n := \dim_F D$.

TS: $n = 1$.

Suppose $n \geq 2$. $|D| = q^n$.

$F^\times \subseteq D^\times$, $\quad Z(D^\times) = F^\times$.

The class equation of $|D^\times|$ gives:

$$|D^\times| = |F^\times| + \sum \left| D^\times : C^\times(a) \right|$$

$$C^\times(a) = \{ d \in D^\times : ad = da \}.$$

$$C(a) = C^\times(a) \cup \{0\}.$$

Note $C(a)$ is a division ring.

$$\underbrace{F \subset C(a)}_{r_a} \underbrace{\subset D}_{t_a} \qquad r_a t_a = n$$

$C(a) \neq D. \quad \therefore t_a > 1.$

$$\Rightarrow \quad q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^{r_a} - 1}$$

$$\Rightarrow \quad q^n - 1 = q - 1 + \sum \Phi_n(q)\, h_n(q)$$

Let Φ_n denote the n^{th} cyclotomic polyn.

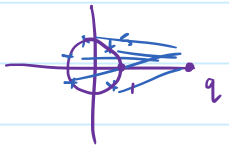
$x^{n-1} = (x^{r_a} - 1)\, \Phi_n(x)\, h(x)$

$$\Rightarrow \quad q^n - 1 = q - 1 + \sum \Phi_n(q)\, h_a(q).$$

n^{th} cyclotomic polyn.
$x^n - 1 = (x^{r_a} - 1)\, \Phi_n(x)\, h(x)$ for some $h(x) \in \mathbb{Z}[x]$ $(\because r_a \neq n)$

$$\Rightarrow \quad \Phi_n(q) \text{ divides } q-1.$$

$$\Rightarrow \quad q-1 \geq |\Phi_n(q)| = \prod_{\substack{\xi \text{ is a} \\ \text{prim. } n^{\text{th}} \text{ root}}} |q - \xi| . \quad \rightarrow\leftarrow$$



$\therefore n = 1.$ ∎

Corollaries. ① A finite domain is a field.
② A finite subring of a division ring is a field.

Example. $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ contains inf. many copies of $\mathbb{C}$.

Defn. Let F be a subfield of a division ring D.
We say D is *algebraic* if every $\alpha \in D$ satisfies a monic polynomial over F.

(Note: F may not be in $Z(D)$.)

Theorem. (Frobenius)
Let D be a division ring such that $\mathbb{R} \subseteq Z(D)$ and D is algebraic over $\mathbb{R}$. Then, $D = \mathbb{R}, \mathbb{C}$, or $\mathbb{H}$.

Proof. Set $n = \dim_{\mathbb{R}}(D)$. (Not assuming $n < \infty$.)

If $n = 1$, then nothing to prove.

Assume $n \geq 2$. Choose $\alpha \in D \setminus \mathbb{R}$.
Then, $\mathbb{R}[\alpha]$ is a proper field extension of $\mathbb{R}$.
$\therefore \mathbb{R}[\alpha] \cong \mathbb{C}$.
Let $T = \mathbb{R}[\alpha]$ and choose $i \in T$ s.t. $i^2 = -1$.
Look at D as a left v.space over T.

T-vec spaces

$D^+ := \{d \in D : di = id\} \supseteq T$, and
$D^- := \{d \in D : di = -id\}$.

$D^+ \cap D^- = 0$.

<u>Claim</u>: $D^+ + D^- = D$.

<u>Proof.</u> Let $a \in D$. $x = ia + ai \in D^+$,

$y = ia - ai \in D^-$.

$$\therefore a = \frac{1}{2i}x + \frac{1}{2i}y \in D^+ + D^- . \quad \blacksquare$$

Note that if $d \in D^+$, then $T[d]$ is a field since d is alg. over $\mathbb{R}$ and hence $\mathbb{C}$.

But $\mathbb{C}$ has no fin. proper ext^n. $\therefore D^+ = T$.

If $D^- = 0$, then $D = T \cong \mathbb{C}$, done.

Assume $D^- \neq 0$. Choose $z \in D^- \setminus \{0\}$.

Define $\mu : D^- \to D^+$,
$x \mapsto xz$.

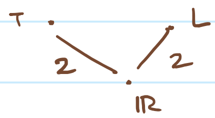
μ is T-linear and injective.

$\therefore \dim_T (D^-) = 1$.

$\therefore \dim_T(D) = 2$. $\therefore \dim_{\mathbb{R}}(D) = 2 \cdot 2 = 4$.

Note $z \notin T$. Put $L = \mathbb{R}[z]$.

$T \cap L = \mathbb{R}$. $\mu(z) = z^2 \in T$.



$\therefore z^2 \in T \cap L = \mathbb{R}$.

If $z^2 \geq 0$, then $z \in \mathbb{R}$. $\rightarrow\leftarrow$

$\therefore z^2 < 0$.

Write $z^2 = -r^2$ for $r > 0$.

Put $j = \frac{z}{r}$ to get $j^2 = -1$.

Conclude $\mathbb{H} = \mathbb{R}[i, j]$
with $ij = -ji$. $\blacksquare$

Lecture (29-03-2022)

29 March 2022 17:26

Given a field F, we wish to construct a division ring s.t. $F = Z(D)$ and $\dim_F D < \infty$.

Defn. Let F be a field, and D a division ring with $Z(D) = F$. We say that D is centrally finite if $\dim_F D < \infty$ and centrally infinite otherwise.

Example. Let k be a field, and $\sigma : k \to k$ an automorphism.
$D = k((x;\sigma))$.
Elements of D are Laurent series $\sum_{j=-m}^{\infty} a_j x^j$.

Multiplication : $xa = \sigma(a)x$.
Then, D is a division ring.

Theorem Set $k_0 := k^\sigma = \{a \in k : \sigma(a) = a\}$.
If σ has infinite order, then $Z(D) = k_0$.
Moreover, $\dim_k D = \infty$ and so $\dim_{k_0} D = \infty$. Thus, D is not centrally finite.

Hilbert's Example : $k = \mathbb{Q}(t)$, $\sigma : k \to k$

$q \mapsto q$ for $q \in \mathbb{Q}$,
$t \mapsto 2t$.

Order of σ is infinite. $\therefore$ $k((x;\sigma))$ is not CF.

Proof. Let $f = \sum_{i=m}^{\infty} a_i x^i \in Z(D)$. Assume $f \neq 0$.

Let j be s.t. $a_j \neq 0$, and $a \in k^\times$ be arbitrary.
Then, $fa = af$ as $f \in Z(D)$.
$$\Rightarrow \sum_{i \geq m} a_i x^i a = \sum_{i \geq m} a a_i x^i$$

$$\Rightarrow \sum_{i \geq m} a_i \sigma^i(a) x^i = \sum_{i \geq m} a_i a x^i.$$

Comparing the coeff of x^j gives $\sigma^j(a) = a$.

But $a \in k^\times$ was arbitrary. As $\mathrm{ord}(\sigma) = \infty$, $j = 0$.

That is, only nonzero coeff possible is a_0.

$\therefore f = a_0 \in k$.

But $xf = fx \Rightarrow \sigma(a_0) = a_0$ or $a_0 \in k_0$.

$\therefore Z(D) \subseteq k_0$. $\supseteq$ is clear.

Thus, $Z(D) = k_0$.

$\dim_k(D) = \infty$ is clear as $\{1, x, x^2, \ldots\}$ are lin. indep. ∎

(Contd) Suppose $\mathrm{ord}(\sigma) = s < \infty$.

$G = \{1, \ldots, \sigma^{s-1}\}$, $k_0 = k^G$.

Recall that k/k_0 is a Gal. ext^n with $\mathrm{Gal}(k/k_0) = G$.

Then,

(1) $Z(D) = k_0((x^s))$,

(2) $K = k((x^s))$

$$\begin{array}{c} k((x^s)) \\ \Big| \text{ Galois} \\ k_0((x^s)) \end{array}$$

(3) $D = K \oplus Kx \oplus \cdots \oplus Kx^{s-1}$.

$$\dim_{k_0((x^s))} D = \dim_{k_0((x^s))} K \cdot \dim_K D$$

$$= s \cdot s = s^2.$$

Proof (1) As before, let $0 \neq f \in Z(D)$, $a_j \neq 0$ appear in f.

Then, $\sigma^j(a) = a \quad \forall a \in k^\times$.

$\Rightarrow \mathrm{ord}(\sigma) \mid j$

$\Rightarrow s \mid j$.

Thus, $f \in k((x^s))$.

Now, $xf = fx \Rightarrow f \in k_0((x^s))$.

$\therefore Z(D) \subseteq k_0((x^s))$. As before $k_0((x^s)) \subseteq Z(D)$.

(2) Straightforward.

(3) Note $D = k((x))$ as a left k-module.

$K = k((x^s))$.

$D = K \oplus Kx \oplus \cdots \oplus Kx^{s-1}$ is clear. ∎

Dickson's Construction

$$\begin{array}{c} K \\ \Big| \quad \text{Galois of order } s \\ F \end{array}$$

$\dim_F K = s$. K is normal and separable.

$G_F(K) = Gal(K/F) =$ Galois group of K over F.

Assume $G_F(K) = \langle \sigma \rangle$.

Fix $a \in F^\times$.

Define the algebra $D := (K/F, \sigma, a)$ is defined as

$$D = K \cdot 1 \oplus K \cdot x \oplus \cdots \oplus K \cdot x^{s-1}.$$

Component wise addition. Multiplication : $x^s = a$,

$x \cdot b = \sigma(b)\, x$.

Then, $\dim_F D = s^2$.

In general, D need not be a division ring.

If $a = 1$ and $s \geq 2$, then

$$\underset{\neq 0}{(1 - x)}\ \underset{\neq 0}{(1 + x + \cdots + x^{s-1})} = 1 - x^s = 0.$$

$\therefore D$ is not a division ring.

Recall: $\begin{array}{c} E \\ \Big| \quad \text{Galois} \\ F \end{array}$

- $x \in E$, then $N_{E/F}(x) = \prod_{\sigma \in G_F(E)} \sigma(x)$.

- $\mu_x : E \to E$
  $e \mapsto ex$ is F-linear and $\det(\mu_x) = N_{E/F}(x)$.

Theorem (Dickson).
Suppose $s = \dim_F(K)$ is a prime number, and $a \in F^\times$.
Then,

$$D = (K/F, \sigma, a) \text{ is a division ring} \iff a \notin N_{K/F}(K^\times).$$

EXAMPLE. $\mathbb{Q}(\sqrt{d}) / \mathbb{Q}$, $s = 2$, $d \in \mathbb{Z}$ square free.

① $d = -m$ for $m \geq 2$.

$\alpha = x + y\sqrt{m}$. $(x, y \in \mathbb{Q}.)$

$N(\alpha) = x^2 + my^2 > 0$.

$\therefore -1 \notin N(\mathbb{Q}(\sqrt{d})^\times)$.

Can take $a = 1$ then.

② $d > 0$.

$\alpha = x + y\sqrt{d}$. $(x, y \in \mathbb{Q})$

$N(\alpha) = x^2 - dy^2$.

Pick $\xi \in \mathbb{Z}$ s.t. ξ is not a square modulo d.

Claim: $\xi \notin N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\mathbb{Q}(\sqrt{d})^\times)$.

Proof. Assume $\xi = N(\alpha)$

for $\alpha = \frac{a}{c} + \frac{b}{c}\sqrt{d}$ with $\gcd(a, b, c) = 1$.

$$\therefore \xi = \frac{a^2}{c^2} - \frac{b^2}{c^2} d$$

$$\Rightarrow c^2 \xi = a^2 - b^2 d \quad \text{——} (*)$$

$$\Rightarrow c^2 \xi \equiv a^2 \mod d.$$

If c is invertible mod d, the $\xi = (a/c)^2 \mod d$

$\to\leftarrow$

Thus, c is divisible by some prime factor p of d.
Looking at $(*)$ shows that $p \mid a$.
But then $p^2 \mid b^2 d$.
But $p^2 \nmid d$. $\therefore p \mid b$.
$\Rightarrow \gcd(a, b, c) > 1$. $\to\leftarrow$

To prove Dickson's result, we will need some facts about simple rings (no proper two sided ideal).

Lemma. D is a division ring $\Rightarrow M_n(D)$ is a simple ring for $n \geq 1$.

Theorem. Let $R^{(\neq 0)}$ be a simple ring. TFAE
(i) R is left Artinian.
(ii) R is semisimple.
(iii) R has a minimal nonzero left ideal.
(iv) $R \cong M_n(D)$ for some $n \geq 1$ and division ring D.

Proof. (ii) $\Rightarrow$ (iv). By Wedderburn – Artin,
$R \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$.
Simplicity forces $k = 1$.
(iv) $\Rightarrow$ (i) is clear.
(i) $\Rightarrow$ (iii) is clear.
(iii) $\Rightarrow$ (ii) Let $\mathfrak{a}$ be a nonzero minimal left ideal in R.
Let
$$B_{\mathfrak{a}} = \sum_{\substack{\mathfrak{a}' \text{ left ideal} \\ \text{s.t. } \mathfrak{a}' \cong \mathfrak{a}}} \mathfrak{a}'.$$

$B_{\mathfrak{a}}$ is clearly a left ideal.
We show $B_{\mathfrak{a}}$ is also a right ideal.
Let $x \in B_{\mathfrak{a}}$ and $r \in R$.
Let $x = x_1 + \cdots + x_k$ for $x_i \in \mathfrak{a}_i \cong \mathfrak{a}$.
Note that $\varphi_i : \mathfrak{a}_i \to \mathfrak{a}_i r$

$x_i \longmapsto x_i r$

is a map of left R-modules.

ψ_i is onto. As ϕ_i is simple,

either $\psi_i = 0$ or ψ_i is an iso.

In the latter case, $\phi_i r \subset B_\phi$.

$\therefore xr \in B_\phi$.

$\therefore B_\phi$ is a two-sided ideal. As R is simple, this forces $B_\phi = R$. $\therefore$ R is a sum of simple modules. $\boxtimes$

Lecture (05-04-2022)

05 April 2022 17:35

Last time: k: field, $\sigma \in \mathrm{Aut}(k)$.

$D = k((x;\sigma))$. $k_0 = k^{\sigma}$.

Thm. (1) $Z(D) = k_0$ if σ has infinite order.

(2) $Z(D) = k_0((x^s))$ if $\mathrm{ord}(\sigma) =: s < \infty$.

Thus, D is centrally finite iff $\mathrm{ord}(\sigma) < \infty$.

$\hookrightarrow \dim_{Z(D)}(D) < \infty$

• K / F Galois. $G = \mathrm{Gal}(K/F) = \langle \sigma \rangle$. $|G| = s$.

$(K/F, \sigma, a)$ - $D := K \cdot 1 \oplus K \cdot x \oplus \cdots \oplus K \cdot x^{s-1}$.

$x^s = a$

$x b = \sigma(b) x$

Theorem A. (1) D is a simple F-algebra.

(2) $C_D(K) = K$. ($C_D(K)$ = centraliser of K in D.)

(3) K is a maximal subfield of D.

(4) $Z(D) = F$.

$F \subset K \cong K \cdot 1 \subset D$.

Moreover, for $u \in F$: $x \cdot u = \sigma(u)\, x = u x$.

$\therefore F \subset Z(D)$, i.e., D is an F-algebra.

Proof. (1) Let I be a nonzero two-sided left ideal of D.

TS: $I = D$.

Pick $z \in I^{\times} = I \setminus \{0\}$.

Write

$$z = b_{i_1} x^{i_1} + b_{i_2} x^{i_2} + \cdots + b_r x^{i_r},$$

where $0 \le i_1 < i_2 < \cdots < i_r \le s-1$,

$b_{i_j} \neq 0 \quad \forall j,$

$r \geq 1$ is the smallest such.

<u>Claim:</u> $r = 1$.

If Claim is true, then $z = b_{i_1} x^{i_1}$.

Then, multiplying with x^{s-i_1} gives

$$z x^{s-i_1} = b_{i_1} a \in I.$$

But $b_{i_1} a$ is a unit. Done.

Proof of Claim: Suppose $r \geq 2$.

$$z = \sum_{j=1}^{r} b_{i_j} x^{i_j}.$$

$$\sigma^{i_1} \neq \sigma^{i_r}.$$

Let $b \in K$ be s.t. $\sigma^{i_1}(b) \neq \sigma^{i_r}(b)$.

$$zb = \left(\sum b_{i_j} x^{i_j}\right) b$$

$$= \sum_{j=1}^{r} b_{i_j} \sigma^{i_j}(b) x^{i_j}.$$

(b_{i_j} & $\sigma^{i_1}(b)$ commute since both are in K.)

$$\sigma^{i_1}(b) z = \sum_{j=1}^{r} b_{i_j} \sigma^{i_1}(b) x^{i_j}.$$

$$\therefore J \ni zb - \sigma^{i_1}(b) z = \sum_{j=2}^{r} b_{i_j} \left(\sigma^{i_j}(b) - \sigma^{i_1}(b)\right) x^{i_j}.$$

nonzero but smaller r. $\rightarrow\leftarrow$

(2) $C_D(K) = \{d \in D : db = bd \quad \forall b \in K\}$.

$K \subseteq C_D(K)$ is clear.

Let $d = b_0 + b_1 x + \cdots + b_{s-1} x^{s-1} \in C_D(K) \setminus \{0\}$.

Let $b \in K$. $bd = db$

$$\Rightarrow \quad b b_i = b_i \sigma^i(b) \quad \text{for all } i$$

Note $b, b_i \in K$.

Thus, if $b_i \neq 0$, then $\sigma^i(b) = b \quad \forall b \in K$.

$\therefore i = 0$.

(3) If $K \subseteq L \subseteq D$ with L a field, then $L \subseteq C_D(K) = K$.

(4) If $t \in Z(D)$, then $t \in C_D(K) = K$

Also, $tx = xt = \sigma(t)x$

$\Rightarrow t = \sigma(t)$

$\Rightarrow t \in F$. ∎

Theorem B. $D \cong M_n(F)$ as an F-algebra $\iff a \in N_{K/F}(K^*)$

(for some $n \geq 1$)

Corollary (Dickson's result)

Let s be a prime.

D is a division ring $\iff a \notin N_{K/F}(K^*)$.

Proof. If $a \in N_{K/F}(F^*)$, then $D \cong M_s(F)$ with s prime.

$\therefore D$ not a div ring.

Assume D is not a division ring. Then, $D \cong M_r(E)$ for some $r \geq 2$.

simple Artin ring

$F = Z(D) = Z(M_r(E)) \cong Z(E)$.

Thus, E is an F-algebra.

$s^2 = r^2 \dim_F E$.

But s is a prime and $r \geq 2$.

Thus, $r = s$ and $\dim_F E = 1$.

$\therefore D \cong M_s(F)$.

By Thm B, $a \in N_{K/F}(K^*)$. ∎

Preliminaries to prove Theorem B.

$B = K[t;\sigma]$.

↳ polynomials with $t \cdot b = \sigma(b) \cdot t$.

B is an integral domain. (Look at lowest order term.)

Exercise. If $I \subseteq B$ is a left ideal, then I is principal.

Sketch. Pick $0 \neq f \in I$ of lowest deg.

Can assume monic by multiplying on left.

Divide ...

$$\dim_K (B/Bf) = (\dim_F K) \deg f.$$

Define $\Theta : K[t;\sigma] \longrightarrow D$ ring map

by $k \longmapsto k$,

$t \longmapsto x$.

Check that this is a well-defined ring map!

Note that Θ is onto. $t^s - a \in \ker(\Theta)$.

Also, $t^s \in Z(K[t;\sigma])$ as $\sigma^s = id_K$.

$\therefore$ $t^s - a$ is a central element and hence,

$B(t^s - a)$ is a two-sided ideal.

Note $\dim_K \left(\dfrac{B}{B(t^s-a)} \right) = s$.

$$\therefore \dim_F \left(\frac{B}{B(t^s-a)} \right) = s^2.$$

Θ is k-linear.

$$\therefore \ker \Theta = B(t^s - a).$$

Proof of Thm B. ($\Leftarrow$) $a \in N_{K/F}(K^\times)$.

$a = N(u)$. Let $d := u^{-1}$. ($u, d \in K^\times$.)

$y := dx \in D$.

$y^2 = dx\,dx = d\,\sigma(d)\,x^2$

$y^3 = d\,\sigma(d)\,x^2\,dx = d\,\sigma(d)\,\sigma^2(d)\,x^3$

$\vdots$

$$\Rightarrow \quad y^i = d\sigma(d)\cdots\sigma^{i-1}(d)\,x^i$$

$$\Rightarrow \quad y^s = d\,\sigma(d)\,\cdots\,\sigma^{s-1}(d)\,x^s = N(d)\,a$$
$$= N(u)^{-1}\,a = 1.$$

For $b \in K$, $\quad yb = dxb$
$$= d\sigma(b)\,x = \sigma(b)\,y.$$

$\{1, y, \ldots, y^{s-1}\}$: lin indep over K.

$$D' = (K/F, \sigma, 1) \subseteq (K/F, \sigma, a) = D.$$

Both have same dim.

$$\therefore \quad D = (K/F, \sigma, 1).$$

$B = K[t; \sigma]$.

$D \cong B/_{B(t^s-1)}$.

$$(t^s - 1) = (t^{s-1} + \cdots + 1)(t-1)$$

$$\Rightarrow \quad B(t^s-1) \subseteq \underbrace{B(t-1)}_{\text{maximal left ideal}}.$$

So, D has a simple left module $M = \dfrac{B}{B(t-1)} \cong K \cong F^s$.

$$\xi : D \longrightarrow \mathrm{End}_F(M)$$
$$d \longmapsto \mu_d : M \to M.$$

ξ is an F-linear ring homomomomorphism.

$\because D$ simple, ξ is 1-1. By dimension check, ξ is onto.

$$\therefore \quad D \cong \mathrm{End}_F(M) = M_s(F).$$

$(\Rightarrow)$ $D \cong M_s(F) \leftarrow$ simple F-algebra.

$E = F^n$ is the unique simple $M_s(F)$-module.

$D \cong B/B(t^s - a)$.

E is a simple D-module.

$\therefore$ B has a max'l left ideal $Bf \supseteq B(t^s - a)$

s.t. $B/Bf \cong F^s$.

By dimension check, we get $\deg f = 1$.

Write $f = t - c$.

$t^s - a \in B(t-c)$.

$a \neq 0 \Rightarrow c \neq 0$.

$$(t^s - a) = (b_{s-1} t^{s-1} + b_{s-2} t^{s-2} + \cdots + b_0)(t - c)$$
$$= b_{s-1} t^s + (b_{s-2} - b_{s-1} \sigma^{s-1}(c)) t^{s-1}$$
$$+ \cdots$$

Compare coefficients from top to iterate and get

$b_{s-1} = 1, \ \ldots, \ a = N(c)$. ∎