Lecture 9 Finite and Algebraic Extensions

Review on ring theory:

(i) Ring and ring homomorphism.

A ring R is a set, together with two monoid structures, called $+, \cdot$, satisfying

A) $(R, +)$ is an abelian group.

its unit element is denoted by 0.

M) $(R, \cdot)$ is a monoid, (commutative or not)

its unit element is denoted by 1.

D) Compatibility between two monoid structures.

$$\begin{cases} a\cdot(b+c) = a\cdot b + a\cdot c \\ (b+c)\cdot a = b\cdot a + c\cdot a \end{cases}$$

Usually, we require $0 \neq 1$. (otherwise, $R = \{0\}$.

If: $a = a\cdot 1 = a\cdot 0 = 0$)

If in M), we require commutativity, then we call R commutative ring.

Theory of comm. ring is the foundation of modern algebraic geometry.

Moreover, in M), we require $(R\setminus\{0\}, \cdot)$ is an abelian group.

Then we call such an R field.

Ex: R is a commutative ring.

$\forall n \geq 1$. define $M_n(R)$ by the usual of matrix addition and multiplication. It is then a noncommutative ring if $n \geq 2$.

Its multiplicative units (= elts which are multiplicative invertible)

$$U(M_n(R)) \stackrel{\Delta}{=} GL_n(R)$$

Most important examples:

$\mathbb{Z}$ and $K[x]$, K a field.

Both are examples of

Def (Euclidean ring)

A commutative ring R is called euclidean, if $\exists$ fn

$$N: R\setminus\{0\} \longrightarrow \mathbb{N}_{\geq 0} \quad \text{satisfying}$$

(i) $N(a \cdot b) = N(a) + N(b)$

(ii) $\forall\, a, b \in R\setminus\{0\}$ with $N(b) \leq N(a)$, $\exists\, q, r \in R$

$b = a \cdot q + r$ with

either $r = 0$ or $N(r) < N(a)$

For $\mathbb{Z}$, $N: \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N}_{\geq 0}$

$a \longmapsto |a|$

For $k[x]$, $N: k[x] \setminus \{0\} \longrightarrow \mathbb{N}_{\geq 0}$

$f(x) \longmapsto \deg(f)$

Definition (ring homo).

A map $\phi: R \longrightarrow S$ between two rings is said ring homo.

if (i) ϕ preserves two monoid structures. i.e $\forall. r_1, r_2 \in R$.

(i) $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$

(ii) $\phi(r_1 \cdot r_2) = \phi(r_1) \cdot \phi(r_2)$

(ii) Ideal

Definition (Ideal)

A subset $I \subseteq R$ is called ideal if

(1) $\forall\, x_1, x_2 \in I, \quad x_1 + x_2 \in I$

(2) $\forall\, x \in I, \ r \in R, \quad r \cdot x \in I$.

(1) + (2) $\Rightarrow$ I is an abelian subgroup

But $(I, \cdot)$ is not nece. a multiplicative submoid,

because 1 is not nece. in I

But, if $1 \in I$, then (2) $\Rightarrow$ $I = R$.

Compare with

Def (Subring)

A subset $S \subseteq R$ is a subring if $(S, +_S)$ abelian subgroup and $(S, \cdot)$ multiplicative submonoid.

$S \xrightarrow{\phi} R$, ϕ the inclusion map is a ring homomorphism.

($\Rightarrow$ $S \hookrightarrow R$ the natural inclusion is a ring homo).

Ex: Show S is a subring $\Longleftrightarrow$ $0, 1 \in S$,

Thus $1 \in S$ for $S \subseteq R$ is a subring.

Lemma: $I \subseteq R$ ideal. Then R/I has natural ring str such $R \xrightarrow{\pi} R/I$ is a ring epimorphism.

Fundamental theorem of ring homo:

$\phi: R \to S$ ring homo. Then

(i) $\ker(\phi) = \phi^{-1}(0) \subseteq R$ is an ideal. $\text{im}(\phi) \subseteq R$ a subring.

(ii) $R/\ker(\phi) \overset{\bar{\phi}}{\simeq} \text{im}(\phi)$ ring iso.

Ideal theory is the most rich part of ring theory.

Def: (Principal ideal ring)

A ring R is called Principal ideal ring if $\forall I \subseteq R$ ideal,

$$I = \{ r \cdot a \mid r \in R \} = (a) \quad \text{for some } a \in R.$$

Ex: $S = \{ a_i \mid i \in I \} \subseteq R$ subset

$(S) \subseteq R$ the ideal generated by S is equal to.

$$\left\{ \underset{\text{finite sum}}{\sum} r_i a_i \;\middle|\; r_i \in R,\ a_i \in S \right\}$$

Prop: Euclean ring is principal ideal ring

Pf: $I \subseteq R$ ideal.

Assume $N(I \setminus \{0\}) \subseteq \mathbb{N}_{\geq 0}$.

$\not\in$

ϕ.

Take $a \in I \setminus \{0\}$. with $N(a)$ minimal in $N(I \setminus \{0\})$

Claim: $I = (a)$.

Take $b \in I$, $N(b) \geq N(a)$. $\Rightarrow \exists q, r \in R$, s.t

$b = aq + r$. $N(r) < N(a)$ or $r = 0$

If $r \neq 0$, then

$$r = qa - b \in I$$

But $N(r) < N(a)$ Contradiction!

Thus $r = 0$. ie $b \in (a)$ as claimed.

#

Cor: $\mathbb{Z}$ and $k[X]$ are principal ideal rng.

Def (irreducible polynomial)

$f(x) \in k[X]$ is called irreducible if

$$f \neq g \cdot h, \text{ where } \deg g \geq 1, \deg h \geq 1.$$

Compare the notion of prime numbers!

Lemma: f irred. $f \mid g \cdot h \Rightarrow$

$$f \mid g \text{ or } f \mid h$$

pf: Assume $f \nmid g$.

Consider $I = (f, g) = \{ af + bg \mid a, b \in k[x] \}$

By Cor, $I = (\tilde{f})$ Thus $f = \tilde{f} \cdot \tilde{g}$

f irred $\Rightarrow$ $\deg \tilde{f} = 0$ or $\deg \tilde{g} = 0$

If $\deg \tilde{g} = 0$, then $f \mid \tilde{f}$

But $\tilde{f} \mid g \Rightarrow f \mid g$ ↯.

Therefore $\deg \tilde{f} = 0$. That is,

$I = k[x]$ (Exercise!)

$\Rightarrow \exists\, a, b \in k[x]$, s.t.

$af + bg = 1$

$\Rightarrow af \cdot h + b \cdot \underbrace{g \cdot h}_{= f \cdot l} = h$

$f(a \cdot h + b \cdot l)$

$\Rightarrow f \mid h$ #

Prop.: ^{0}* $f \in k[x]$. Then $\exists$! factorization

$f = c \cdot f_1^{r_1} \cdots f_s^{r_s}$, where

$c \in K \setminus \{0\}$.

f_i : monic, irreducible

$r_i \geq 1$.

Pf: For f, $c(f) \triangleq$ the coefficient of top degree

Then $f = c(f) \cdot \tilde{f}$, with $\tilde{f}$ monic.

We assume that f is monic in the following.

If f is irreducible, we're done.

Otherwise $f = g \cdot h$, $\deg g, \deg h \geq 1$

But $\deg f = \deg g + \deg h \Rightarrow 1 \leq \deg g < \deg f$

$1 \leq \deg h < \deg f$

Do induction on degree. $\Rightarrow$ Existence of factorization.

Now. assume

$$f_1^{r_1} \cdots f_s^{r_s} = \tilde{f}_1^{\tilde{r}_1} \cdots \tilde{f}_{\tilde{s}}^{\tilde{r}_{\tilde{s}}} \qquad f_i, \tilde{f}_j \text{ irred.}$$

Lemma $\Rightarrow$ up to a permutation of indices.

$$\begin{cases} S = \tilde{S} \\ f_i = \tilde{f}_i \\ r_i = \tilde{r}_i \end{cases}.$$

#

Definition (prime ideal, maximal ideal)

An ideal $I \subsetneq R$ is said to be

- prime, if $a \cdot b \in I \Rightarrow a \in I$ or $b \in I$.

- maximal, if $I \subsetneq J$. J another ideal

$$\Rightarrow J = R.$$

Lemma. $\mathfrak{m} \subsetneq R$ maximal ideal. Then

(i) $\mathfrak{m}$ is prime

(ii) $R/\mathfrak{m}$ is a field.

pf: (i) $a \cdot b \in \mathfrak{m}$, assume $a \notin \mathfrak{m}$.

Consider

$$\mathfrak{m}' = (\mathfrak{m}, a) \supsetneq \mathfrak{m}$$

$\mathfrak{m}$ max $\Rightarrow \mathfrak{m}' = R$

$\Rightarrow \exists\ x \in \mathfrak{m},\ y \in R,$ s.t

$$x + ay = 1$$

$$\Rightarrow \quad \underset{\uparrow}{x} \cdot b + (a \cdot b)\underset{\uparrow}{y} = b$$
$$\mathfrak{m} \qquad \mathfrak{m}$$

$\Rightarrow b \in \mathfrak{m}.$

(ii) Take $\bar{a} \in R/\mathfrak{m}$
$\#$
0

As above, consider

$$R = (\mathfrak{m}, a) \supsetneq \mathfrak{m}$$

$\Rightarrow \exists\ x \in \mathfrak{m},\ y \in R.$ s.t

$$\mathfrak{m} + a \cdot y = 1 \quad \Rightarrow \quad \bar{a} \cdot \bar{y} = 1.$$

$\#$

Ex: $I \subseteq R$, if R/I is field, then I is maximal

Prop: $(f) \subseteq k[x]$ is maximal

$\Leftrightarrow$ f irreducible.

pf: ($\Rightarrow$) If f is not irred, then

$$f = f_1 \cdot f_2, \quad \deg f_i \geq 1$$

$\Rightarrow (f) \subsetneq (f_1) \subsetneq k[x]$ or $(f) \subsetneq (f_2) \subsetneq k[x]$

Thus (f) is not maximal ↯

($\Leftarrow$) $(f) \subsetneq J = (\tilde{f})$

~~Take $a \in J$, $a \notin (f)$~~

$\Rightarrow$

$f = \tilde{f} \cdot \tilde{g}$ $\qquad (f) = (\tilde{f})$ ↯

$\Rightarrow \deg \tilde{f} = 0$ or $\deg \tilde{g} = 0$ ▨

$\Rightarrow \deg \tilde{f} = 0 \Leftrightarrow (\tilde{f}) = k[x]$.

#

$F \subset E$ fields.

- F is a subfield of E

That is F is closed under $(+, -, \times, \div)$

- E is a field extension of F

We can view E as a vector space over F.

$[E:F] \triangleq \dim_F E$.

If $[E:F] < +\infty$, then E is a finite ext. of F.

otherwise, infinite ext.

Pick $\alpha \in E$. Consider the can. morphism

$$\begin{array}{ccc} F[X] & \xrightarrow{\phi_\alpha \,=:\, ev_\alpha} & E \\ \downarrow & & \downarrow \\ \sum_i a_i x^i & \longmapsto & \sum_i a_i \alpha^i \end{array}$$

ϕ_α is the evaluation map at α.

- ϕ_α is a ring homomorphism.
- ϕ_α is also F- vector space hom-morphism.

$\ker(\phi_\alpha) = (f_\alpha) \subseteq F[x]$

f_α monic. Since $\frac{F[x]}{(f_\alpha)} \simeq \mathrm{im}(\phi_\alpha) = F[\alpha] \subseteq E$ (subring)

$\overset{\text{Ex}}{\Rightarrow}$ (f_α) prime ideal.

Case 1. $f_\alpha = 0$. (i.e $\deg f_\alpha = -\infty$)

In this case, we call α is "transcendental" over F.

Case 2. f_α irreducible (i.e $\deg f_\alpha \neq 0$)

In this case, we call α "algebraic" over F.

The poly. f_α is called the <u>irreducible poly. of α over F</u>.

Note that: $F[\alpha] \subseteq E$ is a subfield!

Example: $\mathbb{Q} \subset \mathbb{C}$

- $\alpha = \pi, e, \ldots$ transcendal over $\mathbb{Q}$.
- $\alpha = \sqrt{2}, \sqrt{-1}, \ldots$ algbraic over $\mathbb{Q}$.

The irre. poly of $\sqrt{2}$ over $\mathbb{Q}$: $x^2 - 2 \in \mathbb{Q}[x]$

" " of $\sqrt{-1}$ " : $x^2 + 1 \in \mathbb{Q}[x]$

An ext $F \subset E$ is called algebraic if

$\forall \alpha \in E$, α is algebraic over F.

Ex: $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{C}$

$\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

$\mathbb{Q}(\sqrt{2})$ is algebraic ext of $\mathbb{Q}$:

For $\alpha = a+b\sqrt{2}$:

$b=0, \Rightarrow f_\alpha := x-a$ irred poly

$b \neq 0 \Rightarrow f_\alpha = (x-a)^2 - 2b$ irred poly

Prop: $F \subset E$ finite ext. Then E is alg over F.

pf: Pick any $\alpha \in E$

Consider the subset

$$\{1, \alpha, \alpha^2, \ldots \alpha^n, \ldots\} \subseteq E$$

Since $\dim_F E < +\infty$, it follows that, $\exists\, n \in \mathbb{N}$,

s.t

$\{1, \alpha \dots \alpha^n\}$ linearly dependent

ie, $\exists$ $a_i \in F$, not all zero, s.t

$$\sum_{i=0}^{n} a_i \cdot \alpha^i = 0$$

$\neq 0$

Thus $f(x) = \sum_{i=0}^{n} a_i \cdot x^i \in \ker(\phi_\alpha) \neq 0$

Thus α is algebraic over F. #

But: E alg $F \not\Rightarrow E$ finite over F.

Ex: $\overline{\mathbb{Q}} \triangleq \{\alpha \in \mathbb{C} \mid \alpha$ is algebraic over $\mathbb{Q}\}$

Claim 1: $\overline{\mathbb{Q}}$ is a subfield of $\mathbb{C}$.

It is clear that $\alpha \in \overline{\mathbb{Q}}^{\times}$, then

(i). $-\alpha \in \overline{\mathbb{Q}}$

(ii) $\alpha^{-1} \in \overline{\mathbb{Q}}$

It suffices to show: $\alpha, \beta \in \overline{\mathbb{Q}}$, $\alpha+\beta, \alpha\cdot\beta \in \overline{\mathbb{Q}}$.

For this, consider the tower

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha)(\beta) \overset{\text{def}}{=} \mathbb{Q}(\alpha,\beta)$$

Note $\alpha \in \overline{\mathbb{Q}} \Rightarrow \dim_{\mathbb{Q}} \mathbb{Q}(\alpha) < +\infty$

$= \deg(f_\alpha)$ ← Ex!

$\beta \in \overline{\mathbb{Q}} \Rightarrow$ the irred poly of β over $\mathbb{Q}$

$$f_\beta \in \mathbb{Q}[X],\ 0 \leq \deg f_\beta < +\infty$$

But $f_\beta \in \mathbb{Q}(\alpha)[X]$ and $f_\beta(\beta) = 0$

Thus for $\mathbb{Q}(\alpha)[X] \xrightarrow{\Psi_\beta} \mathbb{Q}(\alpha)(\beta) = \mathbb{Q}(\alpha,\beta)$,

$\ker(\Psi_\beta) \neq 0$ (as $f_\beta \in \ker(\Psi_\beta)$)

Thus $\dim_{\mathbb{Q}(\alpha)} \mathbb{Q}(\alpha,\beta) < +\infty$

($\leq \deg f_\beta$) ← Ex.

It follows from the next prop. that

$$[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(\alpha)]\,[\mathbb{Q}(\alpha) : \mathbb{Q}] < +\infty.$$

Thus $\mathbb{Q}[\alpha, \beta)$ is alg over $\mathbb{Q}$

Since $\alpha+\beta, \alpha, \beta \in \mathbb{Q}(\alpha, \beta)$, they are alg over $\mathbb{Q}$.

#

Claim 2: $\dim_{\mathbb{Q}} \overline{\mathbb{Q}} = +\infty$.

Consider the irred. poly

$$x^n - 2 \in \mathbb{Q}[x]$$

Let $\alpha_n \in \mathbb{C}$ be a solution of

$$x^n - 2 = 0 \quad (\text{Thus } f_{\alpha_n} = x^n - 2$$

Then $\mathbb{Q} \subset \mathbb{Q}(\alpha_n) \subset \overline{\mathbb{Q}} \subset \mathbb{C}$

$$\dim_{\mathbb{Q}} \overline{\mathbb{Q}} \geq \dim_{\mathbb{Q}} \mathbb{Q}(\alpha_n) = \deg f_{\alpha_n} = n \to \infty$$

#.

A tower of fields is a sequence of field extensions.

$$F_1 \subset F_2 \subset \cdots \subset F_n$$

Prop: $F_1 \subset F_2 \subset F_3$. Then $[F_3 : F_1] = [F_3 : F_2] \cdot [F_2 : F_1]$.

pf: Show: $\{x_i\}_{i\in I}$ a basis of F_2 over F_1

$\{y_j\}_{j\in J}$ - - - F_3 over F_2

Then $\{x_i \cdot y_j\}_{\substack{i\in I \\ j\in J}}$ - - - of F_3 over F_1.

It is clear that $\{x_i y_j\}$ spans F_3.

Assume $\sum a_{ij} x_i \cdot y_j = 0$. for a. a. $a_{ij} = 0$.

$a_{ij} \in F_1$

$$\| $$

$$\sum_j \left(\sum_i a_{ij} \cdot x_i\right) y_j$$

$\forall i, x_i \in F_2. \Rightarrow \sum_i a_{ij} \cdot x_i \in F_2$

$\{y_j\}$ F_2-basis $\Rightarrow$ $\sum_i a_{ij} \cdot x_i = 0, \ \forall j.$

$\{x_i\}$ F_1-basis $\Rightarrow$ $a_{ij} = 0. \quad \forall i.$

#

Cor: $F_1 \subseteq F_2 \subseteq F_3$ F_3 finite over F_1

$\Leftrightarrow$ F_3 finite over F_2 and F_2 is finite over F_1.