Lecture 28

(28.0) Let A be a commutative ring. Recall a prime ideal $\mathfrak{p}$ of A is a proper ideal (i.e. $1 \notin \mathfrak{p}$) such that

$$ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \text{ or } b \in \mathfrak{p}$$

Otherwise said $a \notin \mathfrak{p}$, $b \notin \mathfrak{p} \Rightarrow ab \notin \mathfrak{p}$. That is, $S := A \setminus \mathfrak{p}$ is a multiplicatively closed set.

(28.1) Proposition — Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be prime ideals of A. Let $\mathfrak{a}$ be an ideal such that $\mathfrak{a} \subset \bigcup_{i=1}^{n} \mathfrak{p}_i$. Then there is some $j \in \{1, \dots, n\}$ such that $\mathfrak{a} \subset \mathfrak{p}_j$.

Proof — We want to prove

$$\mathfrak{a} \not\subset \mathfrak{p}_j \ \forall j = 1, \dots, n \Rightarrow \mathfrak{a} \not\subset \bigcup_{i=1}^{n} \mathfrak{p}_i \quad \text{[prime avoidance]}$$

This assertion is obviously true for $n = 1$. Assume $n > 1$ and the assertion has been verified for $n-1$. Thus for a fixed $i \in \{1, \dots, n\}$

$$\mathfrak{a} \not\subset \mathfrak{p}_j \ \forall j \in \{1, \dots, n\} \setminus \{i\} \Rightarrow \mathfrak{a} \not\subset \bigcup_{\substack{j=1,\dots,n \\ j \neq i}} \mathfrak{p}_j$$

i.e. we can find $a_i \in \mathfrak{a}$ such that $a_i \notin \mathfrak{p}_j \ \forall j \neq i$.

Now, if $a_i \notin \mathfrak{p}_i$ for some i, we are done (i.e. $\mathfrak{a} \not\subset \bigcup_{\ell=1}^{n} \mathfrak{p}_\ell$ as $a_i \notin \bigcup_{\ell=1}^{n} \mathfrak{p}_\ell$). On the contrary, if $a_i \in \mathfrak{p}_i \ \forall i \in \{1, \dots, n\}$,

we consider the element $a = \sum_{\ell=1}^{n} a_1 \cdots a_{\ell-1} a_{\ell+1} \cdots a_n \in \mathfrak{a}$

For each $i \in \{1, \ldots, n\}$, every summand of a, except $a_1 \cdots a_{i-1} a_{i+1} \cdots a_n$, is in $\mathfrak{p}_i$ (as $a_i \in \mathfrak{p}_i$), and $a_1 \cdots a_{i-1} a_{i+1} \cdots a_n \notin \mathfrak{p}_i$ since $\mathfrak{p}_i$ is prime and none of a_j $(j \neq i)$ are in $\mathfrak{p}_i$.

$\Rightarrow a \notin \mathfrak{p}_i \quad \forall i = 1, \ldots, n$ and we are done. □

(28.2) Proposition – Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals in A and $\mathfrak{p} \subsetneq A$ be a prime ideal. If $\bigcap_{j=1}^{n} \mathfrak{a}_j \subseteq (=) \mathfrak{p}$, then there exists $\ell \in \{1, \ldots, n\}$ such that $\mathfrak{a}_\ell \subseteq (=) \mathfrak{p}$.

Proof – We will prove that $\mathfrak{a}_\ell \notin \mathfrak{p} \quad \forall \ell \in \{1, \ldots, n\} \Rightarrow \bigcap_{j=1}^{n} \mathfrak{a}_j \notin \mathfrak{p}$.

The assumption gives us $a_\ell \in \mathfrak{a}_\ell$ such that $a_\ell \notin \mathfrak{p}$ $(\forall \ell = 1, \ldots, n)$.

Thus $a = a_1 \cdots a_n \in \mathfrak{a}_\ell$ $(\forall \ell)$ and $a \notin \mathfrak{p}$ as $\mathfrak{p}$ is prime.

So $\bigcap_{j=1}^{n} \mathfrak{a}_j \notin \mathfrak{p}$.

Now if $\bigcap_{j=1}^{n} \mathfrak{a}_j = \mathfrak{p}$, then $\mathfrak{a}_\ell \subset \mathfrak{p}$ for some ℓ, by the previous part. Conversely $\mathfrak{p} = \bigcap_{j=1}^{n} \mathfrak{a}_j \subset \mathfrak{a}_\ell$. Hence $\mathfrak{p} = \mathfrak{a}_\ell$.

□

(28.3) Polynomial rings.

Again let A be a commutative ring. The ring $A[x]$ of polynomials in one variable with coefficients from A was defined as

$$A[x] = \left\{ a_0 + a_1 x + \ldots + a_n x^n \;\middle|\; \begin{array}{l} n \in \mathbb{Z}_{\geq 0} \\ a_0, \ldots, a_n \in A \end{array} \right\}$$

Addition is componentwise and multiplication is the usual product of polynomials.

- Universal Property – Given a ring hom $f: A \to B$ (another comm. ring) and $b \in B$, $\exists!$ ring hom

$$\begin{array}{ccc} A[x] & \xrightarrow{ev_{f,u}} & B \\ x & \longmapsto & u \\ \sum_{k=0}^{n} a_k x^k & \longmapsto & \sum_{k=0}^{n} f(a_k) \cdot u^k \end{array}$$

Definition: Given a ring hom $f: A \to B$ between two comm. rings, and $u \in B$, we say u is

- transcendental over A (via f) if $\ker(ev_{f,u}) = (0)$.
- algebraic over A (via f) otherwise

In practice one often drops f if $A \subset B$ is a subring.

eg. $\mathbb{Z} \hookrightarrow \mathbb{R}$, $\sqrt{2}$ is algebraic over $\mathbb{Z}$.

π, e are transcendental.

(28.4) Euclidean algorithm — Given $f, g \in A[x]$, assuming leading term of g is a unit:

$$g = a_0 + a_1 x + \dots + a_\ell x^\ell \quad ; \quad a_\ell \in A \text{ is a unit.}$$

We can prove that f has a unique expression of the form

$$f = q \cdot g + r$$

where degree (r) < degree (g).

Exercise: Show that $K[x]$ is a principal ideal domain, for any field K.

(28.5) Several variables. Let A be a commutative ring, and $n \geq 1$.

$A[x_1, \dots, x_n]$ = ring of polynomials in n variables with coefficients from A.

A typical element $f \in A[x_1, \dots, x_n]$ has the form

$$f = \sum_{\underline{\alpha} = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}} f_{\underline{\alpha}} \, \underline{x}^{\underline{\alpha}} \qquad \text{where } \underline{x}^{\underline{\alpha}} = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$$

finite sum

$f_{\underline{\alpha}} \in A$

Addition and multiplication as usual:

$$\sum_{\underline{\alpha}\in\mathbb{Z}^n_{\geq 0}} f_{\underline{\alpha}}\,\underline{x}^{\underline{\alpha}} \;+\; \sum_{\underline{\beta}\in\mathbb{Z}^n_{\geq 0}} g_{\underline{\beta}}\,\underline{x}^{\underline{\beta}} \;=\; \sum_{\underline{\alpha}\in\mathbb{Z}^n_{\geq 0}} (f_{\underline{\alpha}} + g_{\underline{\alpha}})\,\underline{x}^{\underline{\alpha}}$$

$$\left(\sum_{\underline{\alpha}} f_{\underline{\alpha}}\, x^{\underline{\alpha}}\right)\cdot\left(\sum_{\underline{\beta}} g_{\underline{\beta}}\,\underline{x}^{\underline{\beta}}\right) = \sum_{\underline{\gamma}}\left[\sum_{\underline{\alpha}+\underline{\beta}=\underline{\gamma}} f_{\underline{\alpha}}\, g_{\underline{\beta}}\right]\underline{x}^{\underline{\gamma}}$$

Universal Property. Given a ring hom $f: A \to B$ between two commutative rings A & B; and $b_1, \ldots, b_n \in B$, $\exists!$ ring hom

$$ev_{f;b_1,\ldots,b_n}: A[x_1,\ldots,x_n] \longrightarrow B$$

$$\sum_{\underline{\alpha}} a_{\underline{\alpha}}\, x_1^{\alpha_1}\cdots x_n^{\alpha_n} \longmapsto \sum_{\underline{\alpha}} f(a_{\underline{\alpha}})\, b_1^{\alpha_1}\cdots b_n^{\alpha_n}$$

Again, we say $\{b_1,\ldots,b_n\}$ are <u>algebraically independent</u> (over A via f) if $\operatorname{Ker}(ev_{f;b_1,\ldots,b_n}) = (0)$.

(28.6) Generalization – Monoid ring (and group ring)

Let A be a commutative ring and M be a monoid (i.e. a set with an associative product $M\times M \to M$, $(x,y)\to x\cdot y$ and a neutral element $e\in M$, $e\cdot x = x\cdot e = x \;\; \forall x\in M$).

$$A[M] := \{ f: M\to A \text{ such that } f(x)=0 \text{ for all but finitely many elements of } M\}$$

Ring structure. $(f+g)(x) = f(x)+g(x)$

$$(f \cdot g)(x) = \sum_{y \in M} f(xy^{-1})\, g(y)$$ (necessarily a finite sum as $f, g \in A[M]$)

Verify that $f \cdot g \in A[M]$ (i.e. $(f \cdot g)(x) = 0$ for all but finitely many elements of M.)

$A[M]$ is called the <u>monoid ring</u> (or <u>group ring</u> if M is a group) <u>of M over A</u>

Exercise - • $M = (\mathbb{Z}_{\geq 0}^{n}, +)$; $A[M] = A[x_1, x_2, \ldots, x_n]$

• $M = (\mathbb{Z}^n, +)$; $A[M] = A[z_1^{\pm 1}, \ldots, z_n^{\pm 1}]$

• $M = (\mathbb{Z}/N\mathbb{Z}, +)$; $A[M] = A[x]/(x^n - 1)$

(28.7) Dimension of a ring. Let A be a commutative ring. A chain of prime ideals in A is

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_\ell$$ (ℓ = length of this chain)

$$\dim(A) := \sup_{(\ell \in \mathbb{N})} \{ \ell : \exists \text{ a chain of prime ideals of length } \ell \}$$

e.g. $A = K$ a field has dimension 0.

$A = \mathbb{Z}$ has dimension 1.

$A = \mathbb{C}[x]$ has dimension 1.
↑ or any field

(28.8) Generalization of Euclidean algorithm. – Assume A is a domain together with a function

$$\delta : A \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$$

such that, if $a, b \in A$, non-zero elements ($b \neq 0$), then $\exists\, q, r \in A$ such that

$$a = bq + r \quad \text{with} \quad \delta(r) < \delta(b) \text{ or } r = 0.$$

Such rings are called <u>Euclidean domains</u>.

Examples. – $A = \mathbb{Z}$, $\delta(n) = |n|$

Homework. – $A = \mathbb{Z}[\sqrt{-1}]$, $\delta(z) = z \cdot \overline{z}$ $(\forall\, z \in A)$

Proposition. – A is Euclidean $\Rightarrow$ A is a principal ideal domain.

There are examples of PID's which are non-Euclidean

(e.g. $\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{-19})\right]$