Lecture L1: GCDs and Noetherian Rings

Recall: Last time we defined UFDs and we prove:

Lemma: In a UFD, irreducible elements are prime.

Theorem 1: Any PID is a UFD. In particular, any Euclidean domain is a UFD.

Corollary 1: $\mathbb{Z}$, $K[x]$ (K field) and $\mathbb{Z}[i]$ are UFDs.

The result is stronger (we will see it in a future lecture)

Theorem 2: If R is a UFD, then $R[x]$ is also a UFD.

Corollary 2: For every field K and $n \in \mathbb{N}$, we have $K[x_1, x_2, \ldots, x_n]$ is also a UFD

§51.1 Greatest Common Divisors in UFDs:

Definition: Given R ring and $a, b \in R$, a greatest common divisor between a & b is an element $d = \gcd(a,b) \in R$ satisfying the following properties:

(1) $d \mid a$ and $d \mid b$ in R

(2) if $c \mid a$ and $c \mid b$ in R, then $c \mid d$ in R

⚠ gcd do not always exist for arbitrary ring. If the do, they are well-defined up to multiplication by a unit of R.

Recall: In $\mathbb{Z}$, we can build the $\gcd(n,m)$ from the factorization of n, m.

We show the same idea works in any UFD:

Theorem: In a UFD, gcds exist.

Write
$$n = \pm p_1^{e_1} \cdots p_r^{e_r} \qquad e_1, \ldots, e_r \geq 1 \qquad p_1, \ldots, p_r \text{ distinct primes (positive)}.$$
$$m = \pm q_1^{f_1} \cdots q_s^{f_s} \qquad f_1, \ldots, f_s \geq 1 \qquad q_1, \ldots, q_s \text{ ———————}$$

We assume $p_1 = q_1, \ldots, p_t = q_t$ and the remaining primes are all distinct, meaning $\{p_{t+1}, \ldots, p_r\} \cap \{q_{t+1}, \ldots, q_s\} = \emptyset$. Then
$$\gcd(n,m) = p_1^{\min\{e_1, f_1\}} \cdots p_t^{\min\{e_t, f_t\}}$$

• The same method works for other UFDs.

Let R be a UFD and $a, b \in R \setminus \{0\}$. Write

$$a = u\, p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} \quad \text{and} \quad b = v\, p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}$$

where
- $u, v \in R^\times$
- $p_1, \dots, p_n$ are non-associated primes / irred. elements of R
- $e_1, \dots, e_n, f_1, \dots, f_n \in \mathbb{Z}_{\geq 0}$

Lemma: $\gcd(a,b) := p_1^{\min\{e_1, f_1\}} \cdots\cdots p_n^{\min\{e_n, f_n\}}$ is the greatest common divisor between a & b.

Proof: (1) is clear: $a = d\big(\underbrace{p_1^{e_1 - \min\{e_1, f_1\}} \cdots\cdots p_n^{e_n - \min\{e_n, f_n\}}}_{\in R}\big)$

$$b = d\big(\underbrace{p_1^{f_1 - \min\{e_1, f_1\}} \cdots\cdots p_n^{f_n - \min\{e_n, f_n\}}}_{\in R}\big)$$

(2) is also clear since prime / irreducible elements occurring in the decomposition of c have to be associate to those in the subset $\{p_1 \cdots p_n\}$. Furthermore, the exponent of p_j in c has to be $\leq e_j$ and f_j, so it's $\leq \min\{e_j, f_j\}$. $\square$

§51.2 Noetherian rings:

Let R be a commutative ring.

Definition: We say R is Noetherian (after Emmy Noether) if the following holds:

(Ascending Chain Condition)

Given any ascending chain of ideals in R $\; I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ there exists $n \geq 1$ such that $I_n = I_{n+1} = \cdots$

Non-example: Let R = ring of continuous functions (real-valued) of one (real) variable x.

$$= \{ f : \mathbb{R} \longrightarrow \mathbb{R} \text{ continuous} \}$$

$I_n := \{ f \in R \;:\; f(x) = 0 \;\; \forall x \in [-\tfrac{1}{n}, \tfrac{1}{n}] \}$ for $n = 1, 2, 3, \dots$

As $[-1,1] \supseteq [-\tfrac{1}{2}, \tfrac{1}{2}] \supseteq [-\tfrac{1}{3}, \tfrac{1}{3}] \supseteq \cdots$ we get $I_1 \subseteq I_2 \subseteq I_3 \subseteq I_4 \subseteq \cdots$

Exercise: This chain never stops ie it doesn't stabilize as in the condition defining Noetherian rings.

- Before giving examples of Noetherian rings, we need the following two equivalent ways of proving that a ring R is Noetherian.

Proposition: Assume R is a commutative ring. Then, the following are equivalent:

(1) R is Noetherian.

(2) Given an ideal $I \subseteq R$, there exist finitely many $a_1, a_2, \dots, a_N \in I$ such that $I = (a_1, \dots, a_N)$

(Read: every ideal in R is finitely generated)

(3) Let X be a non-empty set of ideals of R. Then, $\exists\, J \in X$ such that

$$J \subseteq I \ \&\ I \in X \implies J = I.$$

(Read: every non-empty set of ideals in R has an ideal that is maximal with respect to inclusion)

Proof: We show (1) $\Rightarrow$ (3) $\Rightarrow$ (2) $\Rightarrow$ (1)

(1) $\Rightarrow$ (3): We assume R is Noetherian, ie the (ACC) holds.

Let X be a non-empty set of Ideals in R. We argue by contradiction.

Choose $I_1 \in X$. Since I_1 is not maximal in X, $\exists\, I_2 \in X$ with $I_1 \subsetneq I_2$

Repeating the same argument we get an ascending chain of ideals (elements of X)

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$$

This chain does not stabilize since $I_n \subsetneq I_{n+1}$. This contradicts the fact that R is Noetherian. Conclusion: For some $N \geq 1$, $I_N \in X$ is maximal among all elements of X

(3) $\Rightarrow$ (2): Let $I \subseteq R$ be an ideal. Consider the following set of ideals in R

Consider $X = \{ I' \subseteq I \ : I' \text{ is a finitely generated ideal of } R \}$

- $X \neq \emptyset$ since $I' = (0) \in X$.
- Let $I_1 \in X$ be maximal among all ideals from X. Such element exists by (3).

We get
- $I_1 \subseteq I$
- I_1 is finitely generated
- If $I_1 \subseteq I_2 \subseteq I$ & I_2 is a finitely generated ideal, then $I_1 = I_2$.

We claim that $I_1 = I$, hence I is finitely generated.

We argue by contradiction. If $I_1 \subsetneq I$, $\exists\, a \in I \setminus I_1$. Then $I_2 = I_1 + (a)$ satisfies
- I_2 is a finitely generated ideal of R
- $I_2 \subseteq I$

$\Rightarrow I_2 \in X$ & $I_1 \subsetneq I_2$

This contradicts the maximality of I_1 as an element of X. Thus, $I_1 = I$ as we wanted. $\square$

(2) $\Rightarrow$ (1): We check the (ACC) holds for R.

Assume we are given an ascending chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ $(*)$

Take $I = \bigcup_{j\geq 1} I_j \subseteq R$. Then, I is an ideal ($I = \sum_{j\geq 1} I_j$ because $I_n \subseteq I_{n+1}\ \forall n$)

By (2), I is finitely generated, ie $I = (a_1, \ldots, a_N)$ for some finite number of elements $a_1, \ldots, a_N \in I$.

By definition of I $\exists\, k_1, k_2, \ldots, k_N$ st
$a_1 \in I_{k_1}$,
$a_2 \in I_{k_2}$
$\vdots$
$a_N \in I_{k_N}$

Take $M = \max\{k_1, \ldots, k_N\}$. Then, $a_1, a_2, \ldots, a_N \in I_M \subseteq I_{M+1} \subseteq \cdots$

This gives $I \subseteq I_M \subseteq I_{M+1} \subseteq I_{M+\ell} \subseteq I$ $\forall \ell \geq 0$. Hence, $I_M = I_{M+1} = \cdots = I$

We conclude the chain $(*)$ stabilizes $\square$

§51.3 Examples:

(1) Every principal ideal ring is Noetherian

(Recall: R is a principal ideal ring if every ideal I has the form $I = (a)$)
principal ideal

Examples: $R = K$ any field; $\mathbb{Z}$; $K[x]$; $K[\![x]\!]$; $\mathbb{Z}/n\mathbb{Z}$ $n \geq 2$, $\mathbb{Z}[i]$

(2) If $R = K[x_1, x_2, \ldots, x_n, \ldots]$ is a polynomial ring in infinitely many variables, then R is not Noetherian since $I = (x_1, x_2, \ldots)$ cannot be generated by finitely many elements

Reason: Assume $I = (f_1, \ldots, f_r)$ for some $f_1, \ldots, f_r \in R$. By construction, each f_i involves only finitely many variables, so $\exists\, n$ with $f_1, \ldots, f_r \in K[x_1, \ldots x_n]$

$f_i \in I \Rightarrow \exists\, g_1^{(i)}, \ldots, g_{s_i}^{(i)} \in R$ with $f_i(\underline{x}) = \sum_{j=1}^{s_i} g_j^{(i)}(\underline{x})\, x_j$ $(*)$

As before, $\exists\, m \geq n$ such that all polynomials above lie in $K[x_1, \ldots x_m]$.

Evaluating $(*)$ in $x_1 = \cdots = x_m = 0$, we get $f_i(\underline{0}) = \sum_{j=1}^{s_i} g_j^{(i)}(\underline{0}) \cdot 0 = 0$.

Claim: $x_{n+1} \notin (f_1, \dots, f_r)$

We argue by contradiction. Assume $x_{n+1} = \sum_{i=1}^{r} h_i(\underline{x})\, f_i(x_1, \dots x_n)$

↳ involving finitely many variables

Evaluating both sides at $x_1 = x_2 = \cdots = x_n = 0$. we get:

$$x_{n+1} = \sum_{i=1}^{r} h_i(0, \dots, 0, x_{n+1}, \dots)\, \underbrace{f_i(0, \dots, 0)}_{=0} = 0 \quad \text{Contradiction!}$$

(3) Main example will be provided by Hilbert Basis Theorem: R Noetherian $\Rightarrow R[x]$ is Noetherian.

From here we see that $R[x_1, \dots, x_n]$ is Noetherian for each ring R which is Noetherian (Examples: $R = \mathbb{Z}$, K any field) We will see Hilbert Basis Thm in a future lecture.