LESSON 4 - NOETHERIAN DOMAINS AND UNIQUE FACTORIZATION DOMAINS (X-HOUR)

ERAN ASSAF

1. Introduction

Last lesson we recalled properties of ideals and of integral domains, we've proved that the polynomial ring over a field is a Euclidean Domain, and that Euclidean Domains are Principal Ideal Domains. Today, we are going to recall the definition of a Noetherian Domain and a Unique Factorization Domain, show that a Principal Ideal Domain is a Unique Factorization Domain, and in particular classify ideals in polynomial rings over fields.

2. Noetherian Domains

Definition 1. *A ring R is* **Noetherian** *if it satisfies the* **Ascending Chain Condition** *on ideals. i.e. if any increasing chain of ideals*

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$$

becomes stationery (stabilizes), i.e. there exists some N such that for all $n > N$ one has $I_n = I_N$.

Theorem 2. *Let R be a ring. TFAE:*

(1) *R is Noetherian.*
(2) *If Σ is nonempty set of ideals of R, then it contains a maximal element.*
(3) *Every ideal of R is finitely generated.*

(1) $\implies$ (2). : Choose some $I_1 \in \Sigma$. If I_1 is not maximal, there is some $I_2 \in \Sigma$ such that $I_1 \subsetneq I_2$. Proceeding in this way, we produce an infinite increasing chain, which does not stabilize, contradicting (1). Therefore, some I_n is maximal, proving (2).

[(2) $\implies$ (3)]: Let I be an ideal of R, and let Σ be the collection of all finitely generated ideals $J \subseteq I$. Since $0 \in \Sigma$, it is nonempty. Therefore, it contains a maximal element J. If $J \neq I$, let $x \in I \setminus J$. Since $J \in \Sigma$, J is finitely generated, hence so is the ideal $J + xR$, contradicting the maximality of J, hence $J = I$ is finitely generated.

[(3) $\implies$ (1)]: Let $I_1 \subseteq I_2 \subseteq \ldots$ be an increasing chain of ideals. Then $I = \bigcup_{n=1}^{\infty} I_n$ is also an ideal. By assumption, it is finitely generated, say $I = (a_1, \ldots, a_n)$. For every $i = 1, 2, \ldots, n$, since $a_i \in I$, there exists some m_i such that $a_i \in I_{m_i}$. Set $m = \max(m_1, \ldots, m_n)$. Then $a_1, \ldots, a_n \in I_m$, showing that $I \subseteq I_m$, hence $I_k = I$ for all $k \geq m$. $\square$

Corollary 3. *If R is a PID, then R is Noetherian (and every nonempty set of ideals contains a maximal element).*

Proof. Every ideal is generated by a single element, hence finitely generated. $\square$

3. Unique Factorization Domains

Definition 4. *Let R be an integral domain. An element $0 \neq r \in R$ which is not a unit is called* **irreducible** *if whenever $r = ab$ with $a, b \in R$ then either $a \in R^\times$ or $b \in R^\times$. Otherwise, r is called* **reducible**.

Definition 5. *A nonzero element $p \in R$ is called a* **prime** *if the ideal $(p) = pR$ is prime. In other words, p is prime if whenever $p \mid ab$ then either $p \mid a$ or $p \mid b$.*

Definition 6. *Two elements $a, b \in R$ are* **associate** *if there is $u \in R^\times$ such that $a = ub$.*

Proposition 7. *If R is an integral domain, and $p \in R$ is prime, then p is irreducible.*

Proof. Assume $p = ab$ for $a, b \in R$. Then, as p is prime, either $a \in (p)$ or $b \in (p)$. Assume w.l.o.g. that $a \in (p)$, then $a = pu$ for some $u \in R$, hence $1 = ub$, so $b \in R^\times$ is a unit. Therefore, p is irreducible. $\square$

Example 8. *In $\mathbb{Z}$ the irreducible elements are the prime numbers (and their negatives), and a, b are associates iff $a = \pm b$.*

Proposition 9. *If R is a PID, and $p \in R$ is irreducible, then p is prime.*

Proof. Let p be an irreducible element in R. We will show that (p) is maximal, hence prime. Assume $(p) \subseteq I$ for some ideal I. Since R is a PID, $I = (a)$ for some $a \in R$. But $p \in (p) \subseteq (a)$, hence there exists some $b \in R$ for which $p = ab$. Since p is irreducible, either $a \in R^\times$ or $b \in R^\times$. In the former case, $1 = a^{-1}a \in (a)$, hence $I = (a) = R$, while in the latter $a = abb^{-1} = pb^{-1} \in (p)$, hence $(a) = (p)$. It follows that either $I = R$ or $I = (p)$, showing that I is maximal, hence prime. $\square$

Definition 10. *A* **Unique Factorization Domain** *is an integral domain R in which every nonzero element $r \in R$ which is not a unit can be written as a finite product of irreducible elements $p_i \in R$ (not necessarily distinct) $r = p_1 p_2 \cdots p_n$, and this decomposition is unique up to associates. Namely if $r = q_1 q_2 \cdots q_m$ is another factorization into irreducibles, then $m = n$ and (possibly after renumbering) p_i, q_i are associates.*

Example 11. *A field F is a UFD.*

Proof. Every nonzero element is a unit, hence the condition is empty. $\square$

Example 12. *The ring $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ is an integral domain which is not a UFD, as one can see from the factorization $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3$. (Why are $2, 3, 1 \pm \sqrt{5}$ irreducible? How do we know they are not associate?)*

Proposition 13. *If R is a UFD, $p \in R$ is prime $\iff$ p is irreducible.*

Proof. Assume p is irreducible, and $p \mid ab$. Write $a = \prod p_i$ and $b = \prod q_j$ as products of irreducibles, then by uniqueness of decomposition we either have $pu = p_i$, whence $p \mid a$ or $pu = q_j$ whence $p \mid b$. □

Theorem 14. *If R is a Noetherian domain, every nonzero non-unit element can be written as a product of irreducibles.*

Proof. Consider the set $A \subset R$ of nonzero non-units that do not admit a decomposition into irreducible elements, and let $\Sigma = \{(a) : a \in A\}$. If Σ is nonempty, then since it is a nonempty set of ideals and R is Noetherian, it contains a maximal element $(a) \in \Sigma$. Since a is not irreducible, by definition, we can write $a = bc$ for some $b, c \in R$, both of them non-units. In particular, $(a) \subsetneq (b), (a) \subsetneq (c)$. By maximality, it follows that $b, c \notin A$, so we can write $b = p_1 p_2 \cdots p_m$ and $c = q_1 q_2 \cdots q_n$ for some irreducibles p_i, q_j. Therefore $a = p_1 p_2 \cdots p_m q_1 q_2 \cdots q_n$ is a product of irreducible elements, a contradiction. Thus Σ is empty. □

Theorem 15. *Every PID is a UFD. In particular, every Euclidean Domain is a UFD.*

Proof. Let R be a PID. Since R is Noetherian, a decomposition to irreducibles exists. It remains to prove uniqueness of the decomposition $a = p_1 \ldots p_n$. We proceed by induction on the number n of irreducible factors in some factorization. If $n = 1$, $a = p$ is irreducible. Assume $a = qc$ is some other factorization, starting with the irreducible q. Since p is irreducible, and q is not a unit, $c \in R^\times$, and p, q are associates. For the induction step, assume

$$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m, \quad m \geq n$$

where the p_i, q_j are irreducibles. Since $p_1 \mid q_1 \cdots q_m$, and p_1 is irreducible, hence prime, it must divide some q_j. After reordering, we may assume $p_1 \mid q_1$. But then $q_1 = p_1 u$, and as q_1 is irreducible, $u \in R^\times$, showing that p_1, q_1 are associates. Since R is an integral domain, we can cancel out p_1 and remain with

$$p_2 \cdots p_n = u q_2 \cdots q_m = q_2' q_3 \cdots q_m, \quad m \geq n,$$

where q_2' is again irreducible. By the induction hypothesis, $m = n$, and after renumbering each pair p_i, q_i is associate. □

Corollary 16 (The Fundamental Theorem of Arithmetic)**.** *The integers $\mathbb{Z}$ are a UFD.*

Corollary 17. *If F is a field, $F[x]$ is a UFD.*

All the containments below are proper.

$$\text{Fields} \subset \text{Euclidean domains} \subset \text{PID} \subset \text{UFD} \subset \text{Integral domains}$$

Examples are (in order) $\mathbb{Z}, \mathbb{Z}[(1+\sqrt{-19})/2], \mathbb{Z}[x], \mathbb{Z}[\sqrt{-5}]$.

We end with a few corollaries for polynomials over a field.

Corollary 18. *Let F be a field. Then the prime ideals in $F[x]$ are the ideals $P = (f(x))$, where $f(x)$ is an irreducible polynomial. There is a bijection between primes ideals of $F[x]$ and monic irreducible polynomials.*

Corollary 19. *The quotient $F[x]/(f(x))$ is a field $\iff$ $f(x)$ is irreducible.*

Corollary 20. *Every nonzero polynomial $f(x) \in F[x]$ can be written uniquely as $f(x) = ap_1(x)^{n_1} \cdots p_k(x)^{n_k}$ where the $p_i(x)$ are irreducible monic polynomials, and $a \in F^{\times}$.*

4. Summary

We have reviewed the definitions of Noetherian domains and Unique Factorization Domains. We have proved that PIDs are Noetherian (satisfy the ACC). We have shown that any PID is a UFD, and in particular that ideals in polynomial rings over fields correspond to monic irreducible polynomials. In the next lesson we are going to explore the irreducibility of polynomials.