4.3 Lecture 17: The Ascending Chain Condition

It is not true in every integral domain that every non-zero non-unit element is the product of a finite number of irreducible elements. Let R be the subset of $\mathbb{Q}[X]$ consisting of all elements whose constant term is an integer. We can check that R is a subring of $\mathbb{Q}[X]$ (what needs to be checked is that R is closed under polynomial addition, subtraction and multiplication and that R contains the multiplicative identity element of $\mathbb{Q}[X]$). Then R is an integeral domain, since $\mathbb{Q}[X]$ has no zero divisors.

Consider the element X of R (constant term 0). The polynomial X is irreducible in $\mathbb{Q}[X]$, but it factorizes in $\mathbb{R}$, for example as $2 \times \frac{1}{2}X$. The element 2 is irreducible in R, but $\frac{1}{2}X$ is not, since it factorizes (for example) as $2 \times \frac{1}{4}X$ or $3 \times \frac{1}{6}X$. Any factorization of X in R must include one factor that is a rational multiple of X, with the remaining factors being integers. But no rational mutliple of X is irreducible in R, since aX can be written (for example) as $2 \times \frac{a}{2}X$, for any non-zero $a \in \mathbb{Q}$. It follows that X is not the product of (a finite number of) irreducible elements of R.

The theme of this lecture is to identify a property of rings that ensures that every non-zero non-unit element factorizes as a (finite) product of irreducibles. This means that the process of "pulling out" irreducible factors does not continue indefinitely, so that we do not have "failures of factorization" of the kind in the above example.

Recall that an ideal I of a commutative ring with identity R is *principal* if $I = \langle a \rangle$ for some $a \in R$, i.e.

$$I = \{ra : r \in R\}.$$

An integral domain R is a *principal ideal domain* if all the ideals of R are principal. Examples of PIDs include $\mathbb{Z}$ and $F[x]$ for a field F, and all Euclidean domains.

Definition 56. *A commutative ring R satisfies the* ascending chain condition *(ACC) on ideals if there is no infinite sequence of ideals in R in which each term properly contains the previous one. Thus if*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

is a chain of ideals in R, then there is some m for which $I_k = I_m$ for all $k \geqslant m$.

Note: Commutative rings satisfying the ACC are called *Noetherian*, after Emmy Noether (1882-1935), who was among the first people to recognize the significance of this property, and of ideals in general.

Example 57. *The ring R of the example above is not Noetherian.*

An example of an infinite strictly ascending chain of ideals in R is

$$\langle X \rangle \subsetneq \langle \frac{1}{2}X \rangle \subsetneq \langle \frac{1}{4}X \rangle \subsetneq \dots \langle \frac{1}{2^i}X \rangle \subsetneq \dots$$

To see why (for example) $\langle \frac{1}{2}X \rangle \subsetneq \langle \frac{1}{4}X \rangle$ note that the only elements of degree 0 in R are the integers. So $\frac{1}{4}X$ is not a multiple of $\frac{1}{2}X$ in R.

Example 58. *The ACC is satisfied in $\mathbb{Z}$.*

Proof: Let $I_1 \subseteq I_2 \subseteq \dots$ be an ascending chain of ideals in $\mathbb{Z}$. Choose k with $I_k \neq \{0\}$. Then $I_k = \langle n \rangle$ for some positive integer n. Now for an ideal $\langle m \rangle$ of $\mathbb{Z}$ we have $n \in \langle m \rangle$ if and only if $m|n$. Since n has only a finite number of divisors in $\mathbb{Z}$, this means only finitely many different ideals can appear after I_k in the chain.

Theorem 59. *Let R be a PID. Then the ACC is satisfied in R.*

Proof: Let $I_1 \subseteq I_2 \subseteq \dots$ be an ascending chain of ideals in $\mathbb{R}$. Let $I = \cup_{i=0}^{\infty} I_i$. Then

1. I is closed under addition and multiplication, for suppose a and b are elements of I. Then there are ideals I_j and I_k in the chain with $a \in I_j$ and $b \in I_k$. If $m \geqslant \max(j,k)$ then both a and b belong to I_m and so do $a+b$ and ab. So $a+b \in I$ and $ab \in I$.

2. $0 \in I$ since $0 \in I_i$ for each i.

3. Suppose $a \in I$. Then $a \in I_j$ for some j, and $-a \in I_j$. So $-a \in I$. Thus I is a subring of R.

4. Furthermore I is an ideal of R. To see this let $a \in I$. Then $a \in I_j$ for some j. If r is any element of R then $ra \in I_j$ and $ra \in I$. So whenever $a \in I$ we have $ra \in I$ for all $r \in R$. Thus I is an ideal of R.

Now since R is a PID we have $I = \langle c \rangle$ for some $c \in \mathbb{R}$. Since $c \in I$ there exists n with $c \in I_n$. Then $I_n = \langle c \rangle$ and $I_r = \langle c \rangle$ for all $r \geqslant n$. So the chain of ideals stabilizes after a finite number of steps, and the ACC holds in R.

Theorem 60. *Let* R *be a Noetherian integral domain (for example a PID). Then every element of* R *that is neither zero nor a unit is the product of a finite number of irreducibles.*

Proof: Let $a \in R,\ a \neq 0,\ a \notin \mathcal{U}(R)$ (i.e. a not a unit).

1. First we show that a has an irreducible factor. If a is irreducible, this is certainly true. If not then we can write $a = a_1 b_1$ where neither a_1 nor b_1 is a unit. Then $a \in \langle a_1 \rangle$, and $\langle a \rangle \subset \langle a_1 \rangle$. This inclusion is strict for $\langle a \rangle = \langle a_1 \rangle$ would imply $a_1 = ac$ and $a_1 = a_1 b_1 c$ for some $c \in R$. Since R is an integral domain this would imply that b_1 is a unit, contrary to the fact that the above factorization of a is proper.

   If a_1 is not irreducible then we can write $a_1 = a_2 b_2$ for non-units a_2 and b_2 and we obtain

   $$\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle,$$

   where each of the inclusions is strict. If a_2 is not irreducible we can extend the above chain, but since the ACC is satisfied in R the chain must end after a finite number of steps at an ideal $\langle a_r \rangle$ generated by an irreducible element a_r. So a has a_r as an irreducible factor.

2. Now we show that a is the product of a finite number of irreducible elements of R. If a is not irreducible then by the above we can write $a = p_1 c_1$ where p_1 is irreducible and c_1 is not a unit. Thus $\langle a \rangle$ is strictly contained in the ideal $\langle c_1 \rangle$. If c_1 is not irreducible then $c_1 = p_2 c_2$ where p_2 is irreducible and c_2 is not a unit. We can build a strictly ascending chain of ideals:

   $$\langle a \rangle \subset \langle c_1 \rangle \subset \langle c_2 \rangle \ldots$$

   This chain must end after a finite number of steps at an ideal $\langle c_r \rangle$ with c_r irreducible. Then

   $$a = p_1 p_2 \ldots p_r c_r$$

   is an expression for a as the product of a finite number of irreducibles in R.

□