

Lecture 16 (Factorisation and Ascending Chain Conditions)

Unique Prime Factorisation

Proposition 16.1 Let R be an integral domain. Suppose for $n, m \geq 1$,

$$p_1 p_2 \cdots p_n = u q_1 q_2 \cdots q_m,$$

with $p_1, p_2, \dots, p_n, q_1, q_2, \dots, q_m \in R$ primes elements, and u a unit. Then $n = m$, and after renumbering if necessary

$$p_1 \sim q_1, \quad p_2 \sim q_2, \quad \dots \quad p_n \sim q_n.$$

Proof Recall the defining property of primes elements and the fact that in an integral domain prime elements are irreducible. We induct on n , the number of primes terms on the left hand side. Since primes elements are irreducible,

$$p_1 = u q_1 q_2 \cdots q_m,$$

with $p_1, q_1, q_2, \dots, q_m$ prime elements, and u a unit implies $m = 1$ and $p_1 \sim q_1$. So the result is true in the case $n = 1$.

Suppose now $n > 1$ and the result is true for the case $n - 1$.

$$p_1 p_2 \cdots p_n = u q_1 q_2 \cdots q_m,$$

$p_1, p_2, \dots, p_n, q_1, q_2, \dots, q_m$ primes of R , and u a unit. Then $p_n | u q_1 q_2 \cdots q_m$ and p_n prime implies p_n divides some q_i . By renumbering we may assume $p_n | q_m$. Hence since q_m is irreducible and p_n is not a unit, $p_n \sim q_m$, i.e. $p_n = v q_m$ for some unit $v \in R$. So

$$p_1 p_2 \cdots p_n = u v q_1 q_2 \cdots q_{m-1} p_n,$$

Cancelling the factor $p_n \neq 0$ from each side gives

$$p_1 p_2 \cdots p_{n-1} = (u v) q_1 q_2 \cdots q_{m-1},$$

with $p_1, p_2, \dots, p_{n-1}, q_1, q_2, \dots, q_{m-1}$ prime elements and $u v \in U(R)$. By induction we can conclude $n - 1 = m - 1$, i.e. $n = m$, and after a possible renumbering,

$$p_1 \sim q_1, \quad p_2 \sim q_2, \quad \dots \quad p_{n-1} \sim q_{n-1}.$$

We also have $p_n \sim q_n$. So the result is true for the case n if true for case $n - 1$ and true for case $n = 0$. Hence its true for all $n \geq 0$ by mathematical induction. \square

Corollary In a principal ideal domain factorisation into irreducibles is unique.

Proof Recall, in a principal ideal domain irreducibles are prime. \square

Ascending Chain Conditions

We now turn to showing that in a principal ideal domain every $a \neq 0$ which is not a unit is a product of irreducibles.

We can recast irreducibility in terms of ideals.

Recall in an integral domain

$$a|b \Leftrightarrow bR \subseteq aR, \quad a \sim b \Leftrightarrow aR = bR, \quad \text{and} \quad aR = R \Leftrightarrow a \text{ is a unit of } R.$$

Observation 16.2 (Irreducibility in Terms of Ideals) Suppose R is an integral domain.

A non-zero $\pi \in R$ is irreducible if and only if for all $a \in R$, $\pi R \neq R$ and $\pi R \subseteq aR$ implies $aR = \pi R$ or $aR = R$.

An a non-zero $r \in R$ is reducible if and only if $r = xy$ for some $x, y \in R$, with $aR \subsetneq xR \subsetneq R$ and $aR \subsetneq yR \subsetneq R$.

Lemma Suppose R is an integral domain in which some non-zero $a \in R$ is not a unit and cannot be factored into irreducibles. Then we can find an infinite sequence a_0, a_1, a_2, \dots of such elements in R such that

$$a_0R \subsetneq a_1R \subsetneq a_2R \subsetneq \dots$$

Proof Suppose R and $a \in R$ satisfy the conditions of the Lemma. Note the condition $a \in R$ non-zero and not a unit is equivalent to $0 \subsetneq aR \subsetneq R$. We give a recursive definition of an infinite sequence a_0, a_1, a_2, \dots of elements in R , none of which is expressible as product of irreducibles and such that

$$0 \subsetneq a_0R \subsetneq a_1R \subsetneq a_2R \subsetneq \dots \subsetneq R.$$

Set $a_0 = a$.

Now suppose a_1, \dots, a_n have been defined. So a_n is not 0, not a unit and not irreducible. Hence a_n can be factored as $a_n = xy$, with $a_nR \subsetneq xR \subsetneq R$ and $a_nR \subsetneq yR \subsetneq R$. Both x and y cannot be products of irreducibles as their product a_n is not. Set a_{n+1} to be one of the pair which not a product of irreducibles.

□

Definition 16.3 (The Ascending Chain Condition) A commutative ring R is said to satisfy the ascending chain condition for ideals if any ascending chain of ideals

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$$

stabilises, i.e. for some $n \geq 0$, $I_n = I_{n+1} = I_{n+2} = \dots$

Proposition 16.4 If an integral domain R satisfies the ascending chain condition on ideals, every element $a \in R$ with $aR \neq 0, R$ is a product of irreducibles.

Proof This immediate from the Lemma above.

Lemma 16.5 Suppose $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$ is an ascending chain of ideals in a commutative ring R . Then their union $I = \cup I_n$ is an ideal.

Proof We show I is closed under addition, taking negatives, multiplication by elements of R .

Suppose $a, b \in I$ and $r \in R$. Then for some $n, m \in \mathbb{N}$, $a \in I_n$ and $b \in I_m$. Hence for $N = \max\{n, m\}$, $a \in I_n \subseteq I_N$ and $b \in I_m \subseteq I_N$. Because I_N is an ideal $a + b \in I_N \subseteq I$, $(-a) \in I_N \subseteq I$ and $ra \in I_N \subseteq I$.

Proposition 16.6 A principal ideal domainsatisfies the ascending chain condition for ideals.

Proof Suppose $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$ is an ascending chain of ideals in a P.I.D. R . Then the ideal $I = \cup I_n$ is principal. Suppose $I = aR$. Then $a \in I_n$ for some n . Hence for $m \geq n$, $I = aR \subseteq I_n \subseteq I_{n+1} \subseteq \dots \subseteq I = aR$. Hence $I_n = I_{n+1} = I_{n+2} = \dots = I$.

□

Corollary In a principal ideal every $r \neq 0$ is either a unit or a product of irreducibles. \square

We have also proved factorisation into irreducibles is unique in a P.I.D. Putting these facts together we have proved the following.

Theorem 16.7 A principal ideal domain is a unique factorisation domain.

Ascending Chain Conditions

Definition 16.8 An ideal I of a ring commutative ring R with an identity element is said to be finitely generated if there are element $a_1, a_2, \dots, a_n \in R$ such that

$$I = a_1R + a_2R + \dots + a_nR = \{r_1a_1 + r_2a_2 + \dots + r_na_n \mid r_1, r_2, \dots, r_n \in R\}.$$

We then say a_1, a_2, \dots, a_n generate I . Note assuming R has an identity implies that each $a_i \in I$.

Theorem 16.9 A commutative ring with identity R satisfies the ascending chain condition for ideals if and only if every ideal of R is finitely generated.

Proof Suppose every ideal of R is finitely generated. Let

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$$

is an ascending chain of ideals. We show it stabilises.

The union $I = \cup I_n$ of the ascending chain is an ideal of R . So there are elements $a_1, a_2, \dots, a_n \in I$ which generate I . Hence for each i , $a_i \in I_{N_i}$ for some N_i . If we put $N = \max\{N_1, \dots, N_n\}$ then for each i , $a_i \in I_{N_i} \subseteq I_N \Rightarrow a_iR \subseteq I_N$. Hence

$$I = a_1R + \dots + a_nR \subseteq I_N \subseteq I_{N+1} \subseteq I_{N+2} \dots \subseteq I.$$

Hence $I_N = I_{N+1} = I_{N+2} = \dots = I$.

We now show if R has a non-finitely generated ideal the R has an ascending chain of ideals which does not stabilise. Suppose I is a non-finitely generated ideal of R . Let a_1 be any element of I . Set $I_1 = a_1R$. Then $I_1 \subsetneq I$. Choose $a_2 \in I \setminus I_1$. Set $I_2 = a_1R + a_2R$. Then $I_1 \subsetneq I_2 \subsetneq I$. Now choose $a_3 \in I \setminus I_2$ etc. In this way we can construct a strictly ascending chain of ideals of R . \square