Lecture 49

(49.0) Recall - For an integral domain R - we say $a \in R$ is <u>an irreducible element</u> if $(a \neq 0,\ a \notin R^\times)$

$$a = x \cdot y \implies x \text{ or } y \text{ is a unit.}$$

Lemma. If $a \in R$ is such that $P = (a) \subsetneq R$ is a non-zero prime ideal, then a is irreducible.

Proof. Let us assume that $a = xy$ for some $x, y \in R$.

Then $xy \in P = (a)$ and P is a prime ideal

$\implies x \in (a)$ or $y \in (a)$.

Say $x \in (a)$ to fix ideas. Then $x = a \cdot r$ for some $r \in R$.

and $xy = a \implies a = ary$

$\implies a(1 - ry) = 0$.

As $a \neq 0$; and R is a domain, we get $ry = 1$
(since $P \neq (0)$)

i.e. y is a unit. $\square$

(49.1) Recall that we say R is a unique factorization domain; if for any $n \in R$; $n \neq 0$; $n \notin R^{\times}$, we can write $n = p_1 \cdots p_\ell$ — where $p_1, \ldots, p_\ell \in R$ are (not necessarily distinct) irreducible elements. Moreover, this expression of n is <u>unique</u> up to $\begin{cases} \text{permutation of } p_i\text{'s.} \\ \text{scaling } p_i\text{'s by elements of } R^{\times} \text{ (units).} \end{cases}$

<u>Lemma.</u> Assume R is a unique factorization domain, and $a \in R$ $(a \neq 0, a \notin R^{\times})$ is an irreducible element. Then $P = (a) \subsetneq R$ is a prime ideal.

<u>Proof.</u> (T.S.) $xy \in (a) \Rightarrow x \in (a)$ or $y \in (a)$.

Let us write $xy = a \cdot r$ for some $r \in R$.

Let $x = p_1 \cdots p_\ell$ and $y = p_{\ell+1} \cdots p_m$ be (unique) expressions ($p_1, \ldots, p_\ell, p_{\ell+1}, \ldots, p_m \in R$ are irreducible).

[Note: we are <u>excluding</u> the obvious cases when this cannot be done: i.e. we are assuming here that $x, y \notin R^{\times}$, $x \neq 0$; $y \neq 0$]

Since a is an irreducible element, by the uniqueness part of the definition of a U.F.D., $\exists\, j \in \{1, \dots, m\}$ such that

$$a = u \cdot p_j \quad \text{for some unit } u \in R^\times.$$

If $1 \le j \le l$ then $x = a\,(u^{-1} \cdot p_1 \cdots \overset{\text{skipped}}{\widehat{p_j}} \cdots p_l) \in (a)$

Similarly, if $l+1 \le j \le m$ then $y \in (a)$. Hence (a) is a prime ideal. $\square$

For instance, we proved in last lecture that $3 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible, but $(3) \subset \mathbb{Z}[\sqrt{-5}]$ is not a prime ideal. Thus, we obtain that $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain.

(49.2) Revisiting the polynomial ring $K[x]$ where K is a field. —

We already proved, without much difficulty, that

$$N : K[x] \longrightarrow \mathbb{Z}_{\ge 0}$$
$$N = \deg : f \longmapsto \text{degree of } f$$
$$(N(0) = 0)$$

makes $K[x]$ into a <u>Euclidean domain</u>

Following (long) chain of implications gives us unique factorization of polynomials into irreducible ones.

Euclodean Domain $\Rightarrow$ Principal Ideal domain $\Rightarrow$ Unique factorization domain.

Below, we give a direct proof – which is simpler – but applicable to only Euclidean domains.

(49.3) Theorem ($K[x]$ is a U.F.D.) –

Let $f(x) \in K[x]$; $\deg(f(x)) \geq 1$. Then

- $f(x) = f_1(x) \cdots f_\ell(x)$ where $f_1(x), \ldots, f_\ell(x) \in K[x]$ are irreducible polynomials of degrees ≥ 1. (not necessarily distinct)
- the decomposition is unique upto permutation of irreducible factors; and rescaling by $K^\times = K \setminus \{0\}$.

Proof. We prove the first part by induction on $\deg(f)$.

$\deg(f(x)) = 1$: $f(x) = ax + b$ $(a \neq 0)$ is irreducible ✓

$= a\left(x + \frac{b}{a}\right)$

Now assume that every polynomial of degree $\leq n$ can be written as a finite product of irreducible (non-constant) polynomials. Assume $\deg(f(x)) = n+1 > 1$.

$f(x)$ irreducible $\rightsquigarrow$ we are done.

$f(x)$ not irreducible $\Rightarrow f(x) = f_1(x) \cdot f_2(x)$ each of degree $< \deg(f)$. By induction we are done

Now we address uniqueness. If we had

$$f_1(x) \cdots f_\ell(x) = g_1(x) \cdots g_m(x) \quad - (*)$$

where each $f_1, \dots, f_\ell$ and $g_1, \dots, g_m$ is irreducible (non-constant)

Let us assume $\ell \leq m$ to fix ideas.

<u>Induction on ℓ</u> : $\ell = 1$: $f_1(x) = g_1(x) \cdot (g_2(x) \cdots g_m(x))$

irred $\Rightarrow g_1(x)$ is a unit or $(g_2(x) \cdots g_m(x))$ is a unit

$\Rightarrow m = 1$ and $f_1(x) = g_1(x)$.

<u>$\ell > 1$</u> : Write $g_j(x) = q_j(x) \cdot f_1(x) + r_j(x)$ (Euclidean algorithm)

Divide both sides of $(*)$ by $f_1(x)$ to get

$$r_1(x) \cdots r_m(x) = 0$$

$K[x]$ is a domain $\Rightarrow r_j(x) = 0$ for some $1 \leq j \leq m$.

i.e. $g_j(x) = c_j(x) \cdot f_1(x)$

As $g_j(x)$ is irreducible and $f_1(x)$ is not a unit,

$c_j(x)$ is a unit, say $c_j(x) = c_j \in K^\times$. We get

$$f_2(x) \cdots f_\ell(x) = (c_j \cdot g_1(x))\, g_2(x) \cdots \underset{\text{skipped}}{\widehat{g_j(x)}} \cdots g_m(x)$$

And we obtain uniqueness – by induction

i.e. upto permutation and rescaling by $K^\times$; f_i's and g_j's are equal $\square$

(49.4) Greatest Common Divisor in unique factorization domains:

Let R be a U.F.D. and let $a, b \in R$; $a \neq 0, b \neq 0$.

Write: $a = u \cdot p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ • $u, v \in R^\times$

$b = v \cdot p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}$ • $p_1, \ldots, p_n \in R$ are irreducible / prime elements

$e_1, \ldots, e_n, f_1, \ldots, f_n \in \mathbb{Z}_{\geq 0}$.

~~Then~~ $d \overset{\text{def.}}{:=} p_1^{\min(e_1, f_1)} \cdot p_2^{\min(e_2, f_2)} \cdot \ldots \cdot p_n^{\min(e_n, f_n)}$

Then d is a greatest common divisor of a and b; i.e.,

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

(clearly : $a = d \cdot \left(u \cdot p_1^{e_1 - \min(e_1, f_1)} \cdot \ldots \cdot p_n^{e_n - \min(e_n, f_n)}\right)$

$b = d \cdot \left(v \cdot p_1^{f_1 - \min(e_1, f_1)} \cdot \ldots \cdot p_n^{f_n - \min(e_n, f_n)}\right)$).

(2) if $c \mid a$ and $c \mid b$ then $c \mid d$.

(also clear since primes / irreducibles occuring in the decomposition of c then have to be a subset of $\{p_1, \ldots, p_n\}$ and exponent of p_j in c has to be $\leq e_j$ and f_j.)

(49.5) Again, let R be a <u>unique factorization domain.</u> Let $F = F(R)$ be <u>its field of fractions.</u> Recall that

$F(R) = S^{-1}R$ where $S = R \setminus \{0\}$ is <u>the mult. closed set of all non-zero elements of</u> R.

Let $p(x) \in R[x]$. We are going to view $R \subset F$ (subring) and $R[x] \subset F[x]$.
(subring)

Assume that <u>greatest common divisor of coefficients of $p(x)$ is 1.</u> Meaning - in other words - if we write

$p(x) = c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0$;

$c_0, c_1, \dots, c_n \in R$. Then $d \mid c_j$ for every $0 \leq j \leq n$

implies $d \in R^\times$ (is a unit).

Definition : $p(x) \in R[x]$ is said to be primitive if

$\gcd(\text{coefficients of } p(x))$ is 1.

Lemma (Gauss) If R is a U.F.D. and $p(x) \in R[x]$

is a primitive polynomial. Then :

$p(x)$ is irreducible in $R[x]$ if, and only if

$p(x)$ is irreducible in $F[x]$.

Proof. $(\Rightarrow)$ = "difficult part" :

Assume $p(x) \in R[x]$ is irreducible. Hence $\deg(p(x)) = n \geq 1$.

($\deg(p) = 0$ and primitive $\Rightarrow p \in R^\times$ is a unit.)

To get a contradiction, let us assume $p(x) = A(x) \cdot B(x)$

for some $A(x), B(x) \in F[x]$: $\deg(A(x)) = k \geq 1$

$\deg(B(x)) = n - k \geq 1$

Clearing the denominator, we can find some $d \in R \setminus \{0\}$

s.t. $(*)$: $\boxed{d \cdot p(x) = a(x) \cdot b(x)}$; $a(x), b(x) \in R[x]$.

$\left(\begin{array}{l} a(x) = r \cdot A(x) \\ b(x) = s \cdot B(x) \\ \text{for some } r, s \in F. \end{array} \right)$

<u>Claim</u> : R.H.S. of $(*)$ is divisible by d.

<u>Proof</u> : If d is a unit then there is nothing to prove. Otherwise, we can write

$d = p_1 \cdots p_\ell$ where $p_1, \dots, p_\ell \in R$ are irreducible / prime elements.

Take $P_1 = (p_1) \subsetneq R$ prime ideal (see Lemma 49.1 above).

Consider $(*)$ modulo P_1 :

$$0 = \left[\sum_{i=0}^{k} (a_i \bmod P_1) x^i \right] \cdot \left[\sum_{j=0}^{n-k} (b_j \bmod P_1) x^j \right]$$

But $\left(R/P_1\right)[x]$ is an integral domain. So, either the 1st or the second term above is 0. i.e.,

Either $a_i \in P_1 \quad \forall \; 0 \leq i \leq k$

Or $b_j \in P_1 \quad \forall \; 0 \leq j \leq n-k$.

both terms in $R[x]$.

Thus we get $(p_2 \cdots p_\ell) \cdot p(x) = \left(\dfrac{a(x)}{p_1} \right) \cdot b(x)$

or the other way around

... continue ... to get $p(x) = \left(\dfrac{a(x)}{p_{i_1} \cdots p_{i_r}} \right) \cdot \left(\dfrac{b(x)}{p_{i_{r+1}} \cdots p_{i_\ell}} \right)$ in $R[x]$

$\square$

(49.6) Theorem. — R is a unique factorization domain

$\Longrightarrow$ $R[x]$ is a unique factorization domain.

Proof. — Let us begin by showing that every $p(x) \in R[x]$ (not a unit, non-zero) can be written as a product of irreducible factors. To begin with, we write

$p(x) = \alpha \cdot \bar{p}(x)$ where $\alpha \in R$ is the gcd of the coefficients of $p(x)$; and $\bar{p}(x)$ is primitive

Since $\alpha \in R$ can be written (uniquely) as a finite product of irreducible elements of R; and they remain irreducible in $R[x]$, it is enough to prove our desired statement for primitive polynomial $\bar{p}(x)$.

Assuming $\bar{p}(x)$ is not a unit, we know $\deg(\bar{p}(x)) \geq 1$.

As $F[x]$ is a unique factorization domain, we can write

$\bar{p}(x) = A_1(x) \cdots A_r(x)$ uniquely as a product of irreducible polynomials in $F[x]$.

$\Longrightarrow$ $\bar{p}(x) = a_1(x) \cdots a_r(x)$ in $R[x]$; and for each

(see last page)

$j \in \{1, \ldots, r\}$: $a_j(x) = \lambda_j A_j(x)$

some elt. of $F^\times$.

Since $\overline{p}(x)$ is primitive; so must be each $a_1(x), \dots, a_r(x)$

(because: if $d \in R$ divides all the coefficients of $a_j(x)$, then from $\overline{p}(x) = a_1(x) \cdots a_r(x)$; it divides all the coefficients of $\overline{p}(x)$, hence $d \in R^\times$.)

Thus, using Gauss' Lemma, each $a_j(x)$ is irreducible in $R[x]$ and we are done with the existence of factorization.

<u>Uniqueness</u>: Again we are assuming that $\overline{p}(x) \in R[x]$ is a primitive polynomial, $\deg(\overline{p}(x)) \geq 1$. Assume we have two factorizations: $\overline{p}(x) = a_1(x) \cdots a_r(x) = b_1(x) \cdots b_s(x)$

Each $a_1(x), \dots, a_r(x)$; $b_1(x), \dots, b_s(x)$ – irreducible in $R[x]$ and <u>primitive</u>, hence irreducible in $F[x]$ (Gauss' Lemma).

As $F[x]$ is a U.F.D., we get $r = s$ and (after relabelling) (for any $i \in \{1, \dots, r\}$):

$b_i(x) = \frac{r_1}{r_2} \cdot a_i(x) \implies r_2 \cdot b_i(x) = r_1 \cdot a_i(x)$.

for some $r_1, r_2 \in R \setminus \{0\}$. As both $a_i(x)$ and $b_i(x)$ are primitive, we get that r_1 & r_2 have same irreducible factors

$\implies r_2 = u \cdot r_1$ for a unit $u \in R^\times$.

Hence for each $i \in \{1, \ldots, r\}$:

$$b_i(x) = u_i \, a_i(x) \quad \text{for } u_i \in R^\times.$$

and the uniqueness part follows. $\square$