Lec 11/9

Friday, November 9, 2018 11:30

R is a UFD if every nonzero non-unit element factors "uniquely" into a finite product of irreducible elts. (up to shuffling about & multiplying units.)

(irreducible $\Leftrightarrow$ $a = uv \Rightarrow$ either u or v is unit).

In a UFD, $A \in R$ irred $\Leftrightarrow$ $(a) \subsetneq R$ is a non-zero prime ideal.

$$\begin{array}{ccc} \text{PID} & \Longrightarrow & \text{UFD} \\ \Uparrow & & \\ \text{Euclidean} & & \end{array}$$

main examples: $K[x_1, \dots, x_n]$ (K: a field)

$R = K[x]$ is euclidean w/ $N : R \longrightarrow \mathbb{Z}_{\geq 0}$, $f(x) \longmapsto \deg(f)$ (K: a field)

hence every $f(x) \in K[x]$ factors uniquely into irreducible poly-s.

$(K[x])^\times = K^\times$

Suppose $\deg(f) \geq 1$. f irreducible $\Rightarrow$ we are done.

otherwise $f = f_1 f_2$ (smaller degree) use induction

<u>Uniqueness</u> $f = f_1 \cdots f_k = g_1 \cdots g_\ell$ (say $k \leq \ell$)

<u>induct on k</u> : $k = 1$ ✓

otherwise divide by f_1 : $0 = r_1 \cdots r_\ell \Rightarrow r_j = 0$ for some j (remainders $g_j = f_1 f_j + r_j$)

$\Rightarrow g_j = c \cdot f_j$ for some $c \in K^\times$.

Greatest Common Divisor in UFD:

R: UFD. $a, b \in R$. $a = u\, p_1^{e_1} \cdots p_\ell^{e_\ell}$

$b = v\, p_1^{f_1} \cdots p_\ell^{f_\ell}$ $\quad e_i, f_j$ could be zero.

$$d = \gcd(a,b) = p_1^{\min(e_1,f_1)} \cdots p_\ell^{\min(e_\ell,f_\ell)}$$

Pf is easy.

Theorem: R : UFD $\Longrightarrow$ $R[x]$: UFD.

Cor: $K[x_1, \dots, x_n]$ is UFD.

(we will use $K[x]$ is UFD.)

Let $F = F(R)$ be its field of fractions.

i.e. $F = S^{-1}R$ for $S = R \setminus \{0\}$.

Definition: A polynomial $p(x) \in R[x]$ is called primitive if coefficients of $p(x)$ generate the unit ideal $((1) = R)$

eg: every monic polynomial is primitive.

Gauss's Lemma: if $p(x) \in R[x]$ primitive (and R is UFD) then

$p(x)$ irreducible in $R[x] \iff p(x)$ irreducible in $F[x]$.

Pf $\quad R \overset{\text{subring}}{\subset} F$. $R[x] \overset{\text{subring}}{\subset} F[x]$

($\Longleftarrow$) obvious

($\Longrightarrow$) Let $p(x) \in R[x]$ be an irred. element.

So $\deg(\underset{n}{\underset{\shortparallel}{p(x)}}) \geq 1$ ($\deg(p(x)) = 0$ & p primitive $\Rightarrow$ $p \in R^\times$).

Assume $p(x) = A(x)B(x)$ where $A(x), B(x) \in F[x]$, $\underset{k}{\underset{\shortparallel}{\deg(A(x))}}$, $\underset{n-k}{\underset{\shortparallel}{\deg(B(x))}} \geq 1$

Let $d \in R \setminus \{0\}$ s.t. $\underbrace{dp(x) = a(x)\,b(x)}_{(*)}$ & $a(x), b(x) \in R[x]$.

Claim: d divides $a(x)\,b(x)$. If $d \in R^\times$ there is nothing to prove. o.w. $d = p_1 \cdots p_\ell$ $\leftarrow$ irreducible elements.

$P_1 = (p_1)$ is a prime ideal. $(*) \Rightarrow \left[\sum_{i=0}^{k} (a_i \bmod P_1) x^i\right]\left[\sum_{j=0}^{n-k} (b_j \bmod P_1) x^j\right] = 0$.

in $(R/P_1)[x]$ which is a domain

So either $a(x) \equiv 0 \bmod P_1$ or $b(x) \equiv 0 \bmod P_1$.

So $(*) \Rightarrow p_2 \cdots p_\ell \cdot p(x) = \left(\frac{a(x)}{p_1}\right) b(x)$ in $R[x]$.

repeat the argument w/ P_2, etc.

So $$p(x) = \left(\frac{a(x)}{p_{i_1} \cdots p_{i_r}}\right)\left(\frac{b(x)}{p_{i_{r+1}} \cdots p_{i_\ell}}\right).$$

both in $R[x]$.

So $P(x) = A(x)B(x) = (rA(x))\,(r^{-1}B(x))$ for some $r \in F$.

both in $R[x]$

Theorem: R: UFD $\Rightarrow$ $R[x]$: UFD

Pf To prove: given $p(x) \in R[x]$ not a unit, non-zero, we can write $p(x)$ as a finite product of irreducible elements of $R[x]$.

Write $p(x) = \alpha\, \bar{p}(x)$ where $\alpha = \gcd$ (coefficients of $p(x)$) and $\bar{p}(x)$ is primitive.

$\alpha \in R$ (UFD) so $\alpha = \alpha_1 \cdots \alpha_\ell$ uniquely, so it is sufficient to assume $p(x)$ is primitive.

$p(x) = A_1(x) \cdots A_r(x)$ (factorization into irreducible polynomials in $F[x]$). Gauss's Lemma says

$p(x) = a_1(x) \cdots a_r(x)$ in $R[x]$. $\underset{\shortparallel}{\overset{R}{\text{Ideal}}}$ generated by coeffs $p(x) \subset$ ideal generated by coeffs of a_i

So each a_i is primitive, irreducible in $F[x] \Rightarrow$ irreducible in $R[x]$ (Gauss's lemma again).

Existence ✓

Read: Uniqueness in notes online