Lec 11/13

Tuesday, November 13, 2018 11:29

Unique Factorization Domains:

up to permutation & scaling by units.

R is UFD if every non-zero non-unit element can be written "uniquely" as a product of irreducible elements

$x \in R \setminus (\{0\} \cup R^\times)$ is irreducible if $x = ab \Rightarrow$ either a or b is a unit.

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

UFD

Sometimes in UFD's irreducible elements are also called prime elements.

$$\gcd\left(u\, p_1^{k_1} \cdots p_\ell^{k_\ell},\ v\, p_1^{r_1} \cdots p_\ell^{r_\ell}\right) = p_1^{\min(k_1, r_1)} \cdots p_\ell^{\min(k_\ell, r_\ell)}.$$

Gauss Lemma

- $p(x) \in R[x]$; $\deg(p(x)) \geq 1$, gcd(coefficients) $= 1$.

  Suppose $p(x) = A(x)\,B(x)$ where $A(x), B(x) \in F[x]$ where F = field of fractions of R.

  then $p(x) = a(x)\,b(x)$ where $a(x), b(x) \in R[x]$.

  ($a(x) = \lambda A(x)$ and $b(x) = \lambda^{-1} B(x)$ for some $\lambda \in F$)

Cor.1: R ufd $\Rightarrow$ R[x] ufd.

	(1)	(2)	(3)
R noetherian $\Rightarrow$	R/I noetherian.	Subring of R need not be noetherian.	R[x] Noetherian (Hilbert)
R UFD $\Rightarrow$	R/I need not be UFD.	Subring of R need not be UFD.	R[x] UFD. (Gauss)

$\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

ψ

3 is irreducible but (3) is not a prime ideal.

$\Downarrow$

3 is irreducible but (3) is not a prime ideal.

$\cong \mathbb{Z}[x] / (x^2+5)$ (1)

UFD since field

$\mathbb{Z}[\sqrt{-5}] \underset{\text{subring}}{\subset} \mathbb{C}$ (2)

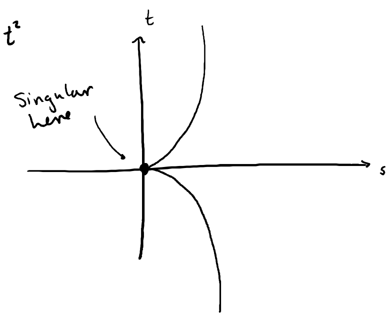
Another example of (2): $K[x]$ is a UFD. (field)

$R = \{ f(x) \in K[x] \mid f'(0) = 0 \text{ i.e. if } f(x) = a_0 + a_1 x + \cdots + a_n x^n \text{ then } a_1 = 0 \} \underset{\text{subring}}{\subset} K[x]$

R is not a UFD. x^2 is irreducible. $(x^2) \ni x^6 = x^3 \cdot x^3$ but $x^3 \notin (x^2)$.

$$R = \text{image of } \begin{aligned} K[s,t] &\longrightarrow K[x] \\ s &\longmapsto x^2 \\ t &\longmapsto x^3 \end{aligned}$$

$s^3 = t^2$



Cor 2 of Gauss Lemma: Eisenstein Criterion for Irreducibility.

(sufficient condition for checking if a polynomial in $\mathbb{Z}[x]$ is irreducible).

Let $f(x) \in \mathbb{Z}[x]$.

Hypotheses:

(1) $\deg(f(x)) \geq 1$.

(2) $\gcd(\text{coefficients of } f(x)) = 1$.

(3) if $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ then there is a prime $p \in \mathbb{Z}_{\geq 2}$

such that $p \nmid a_n$, $p \mid a_i \ \forall i \in \{0, \dots, n-1\}$, and $p^2 \nmid a_0$.

Conclusion: $f(x)$ is irreducible.

eg $f(x) = x^2 + 4x + 2$ is irreducible (take $p=2$)

$= (x+2)^2 - 2 = 0 \Rightarrow$ means $x = -2 \pm \sqrt{2}$

If $f(x) = (x-\alpha)(x-\beta)$ for some $\alpha, \beta \in \mathbb{Q}$ then $f(\alpha) = f(\beta) = 0$; i.e. $\sqrt{2} \in \mathbb{Q}$.

Observation: for any $p(x) \in \overset{\text{field}}{K}[x]$, $p(x)$ is divisible by $(x-\alpha)$ for some $\alpha \in K \iff p(\alpha) = 0$.

Euclid: $p(x) = (x-\alpha)\, q(x) + r(x)$, $r(x)$ is a constant

So $p(\alpha) = 0 \iff r = 0$.

Exercise: $p(x)$ is div. by $(x-\alpha)^2 \iff p(\alpha) = 0,\ p'(\alpha) = 0$.

Proof: Assume $f(x) = g(x)h(x)$ (over $\mathbb{Z}$) with $g(x) = b_k x^k + \dots + b_0$, $h(x) = c_\ell x^\ell + \dots + c_0$.

$k + \ell = n = \deg(f)$, $k, \ell, n \geq 1$. We want to get a contradiction.

- $a_0 = b_0 c_0$. $p^2 \nmid b_0 c_0$ but $p \mid b_0 c_0$ so p divides b_0 or c_0 but not both.

  Say $p \mid c_0$ but $p \nmid b_0$.

- the other extreme: neither b_k or c_ℓ is divisible by p.

$$\underset{\substack{\text{not}\\ \text{div by } p}}{c_\ell x^\ell} + c_{\ell-1}x^{\ell-1} + \cdots + c_1 x + \underset{\text{div by } p}{c_0}$$

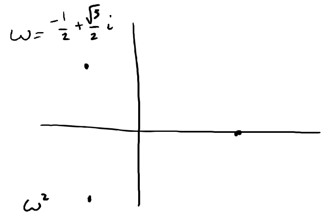
there is r
s.t. $c_0, \dots, c_{r-1} \equiv 0 \mod p$ $\quad (r \leq \ell < n)$.
but $c_r \not\equiv 0 \mod p$.

now $a_r = \underbrace{b_0 c_r}_{\text{not} \equiv 0 \bmod p} + \underbrace{b_1 c_{r-1} + \dots + b_r c_0}_{\text{all} \equiv 0 \bmod p} \not\equiv 0 \mod p$. Contradiction.

Eisenstein criterion is true in general UFD also.

Examples:

$f(x) = x^2 + x + 1 = \dfrac{x^3-1}{x-1}$



and so roots of $f(x)$ are ω, ω^2 so $f(x)$ is irreducible over $\mathbb{Q}$.

$g(x) = f(x+1) = (x+1)^2 + (x+1) + 1 = x^2 + 3x + 3 \Rightarrow$ eisenstein w/ $p=3 \Rightarrow g(x)$ irreducible.

Same trick works for $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$

Eisenstein criterion works for $f(x+1)$ w/ prime p.