Lecture LV: More on UFDs, Eisenstein's Criterion for Irreducibility

§55.1 Summary on UFDs:

Recall: Let R be an integral domain

- $a \in R$ with $a \neq 0$, $a \notin R^\times$ is **irreducible** if $a = xy \Rightarrow x \in R^\times$ or $y \in R^\times$.
- $a \in R$ _____ is prime if $xy \in (a) \Rightarrow x \in (a)$ or $y \in (a)$

Lemma: a prime $\Rightarrow a$ is irreducible

- R is a UFD (unique factorization domain) if every non-zero, non-unit element can be written uniquely as a finite product of irreducible elements of R

That is for every $a \in R$, $a \neq 0$, $a \in R^\times$ there exist irreducible elements $p_1, \dots, p_r$ (not necessarily distinct) so that

$$a = p_1 \cdots p_r \qquad \text{(existence of factorization)}$$

Moreover if $a = q_1 \cdots q_k$, where $q_1, \dots, q_k \in R$ are also irreducible, then $k = l$ and there is a permutation σ of $\{1, \dots, l\}$ and units $u_1, \dots, u_l \in R^\times$ such that

$$q_i = u_i p_{\sigma(i)} \qquad \forall i \in \{1, \dots, l\} \qquad \text{(uniqueness of factorization)}$$

Basic facts about UFDs: Let R be a UFD

(1) $a \in R$ is irreducible $\Leftrightarrow (a) \subsetneq R$ is a non-zero prime ideal

(2) **Gauss's Lemma**: Let $p(x) \in R[x]$ $\deg p(x) \geq 1$ be such that

greatest common divisor of coefficients of $p(x) = 1$ (p is primitive)

Let $F = F(R)$ be the field of fractions of R. If there exists a factorization over F:

$$p(x) = A(x) B(x) \quad \text{where } A(x), B(x) \in F[x] \text{ have degree} \geq 1,$$

then $p(x) = a(x) b(x)$ where $a(x), b(x) \in R[x]$ and $\deg(a) = \deg(A)$, $\deg(b) = \deg(B)$

In fact $\exists \lambda \in F \setminus \{0\} = F^\times$ with $a(x) = \lambda A(x)$ & $b(x) = \lambda^{-1} B(x)$.

(3) Consequence of Gauss's Lemma and the fact that $K[x]$ is a UFD for any field K is

$$\boxed{R \text{ UFD} \Rightarrow R[x] \text{ UFD}}$$

Examples: $\mathbb{Z}[x_1, \dots, x_n]$ is a UFD,

given K field, we have $K[x_1, \dots, x_n]$ is a UFD.

Next, we show that UFDs & Noetherian domains are not related by inclusion:

Theorem 1: UFD $\not\subseteq$ Noetherian domains

Proof: If K is a field, then $R = K[x_1, x_2, \dots]$ is not Noetherian but it is a UFD

Claim 1: R is not Noetherian

Pf/ $I = (x_1, \dots, x_n, \dots)$ is not a finitely generated ideal, as we saw in Lecture 32.

Claim 2: R is a UFD.

Pf/ Pick $f \in R$, $f \neq 0$ & $f \notin R^\times$. Then $\exists\ n \geq 1$ st. $f \in K[x_1, \dots x_n]$

Since $K[x_1, \dots x_n] \subseteq R$ is a subring, $f \notin R^\times \Rightarrow f \notin K[x_1, \dots x_n]^\times = K^\times$

Since $K[x_1, \dots x_n]$ is a UFD $\exists\ f_1, \dots, f_r \in K[x_1, \dots, x_n]$ irreducible

s.t. $f = f_1 \cdots f_r$.

Q1: Why is f_i irreducible in R $\forall$ all i?

Q2: Why is this factorization in R unique (up to associates)?

A1: Assume $f_i = g_i h_i$ in R. Then $\exists\ m \geq n$ such that

$f_i, g_i, h_i \in K[x_1, \dots x_m]$.

Claim: $m = n$.

Pf/ Assume $m > n$: $K[x_1, \dots, x_{m-1}, x_m] = \underbrace{K[x_1, \dots, x_{m-1}]}_{\text{domain}}[x_m]$, so we

can take $\deg_{x_m}$ of $f_i = g_i h_i$ in $K[x_1 \dots x_{m-1}][x_m]$ and use the fact that

$\deg_{x_m}$ is additive with respect to multiplication:

$$0 = \deg_{x_m} f_i = \underbrace{\deg_{x_m} g_i}_{\geq 0} + \underbrace{\deg_{x_m} h_i}_{\geq 0} \Rightarrow \deg_{x_m} g_i = \deg_{x_m} h_i = 0$$

ie $g_i, h_i \in K[x_1, \dots, x_{m-1}]$

By induction on $m - n \geq 0$ we conclude $g_i, h_i \in K[x_1, \dots, x_n]$ ie $m = n$. ☐

Since $f_i \in K[x_1, \dots, x_n]$ is irreducible, we get $g_i \in K[x_1, \dots, x_n]^\times = K^\times \subset R^\times$ or

$h_i \in K^\times \subseteq R^\times$

Conclude: f_i is irreducible in $R^\times$ $\forall i = 1, \dots, r$.

A2: If $f = g_1 \cdots g_r = h_1 \cdots h_s$ with $g_i, h_j \in R$ irreducible $\forall i, \forall j$
Then $f \in K[x_1, \dots x_n]$ for some n implies by the proof of Claim above that $g_i, h_j \in K[x_1, \dots, x_n]$ $\forall i, j$.
Since $K[x_1, \dots x_n] \subseteq R$ subrings, we conclude g_i, h_j are irreducible in $K[x_1, \dots, x_n]$
Thus, because $K[x_1, \dots, x_n]$ is a UFD we get $r = s$ & up to relabeling, $\exists \lambda_1, \dots, \lambda_r \in K^\times \subseteq R^\times$ s.t. $g_i = \lambda_i h_i$.
Conclusion: The factorization in R is unique.

Theorem 2: Noetherian domains $\not\Leftarrow$ UFDs

Proof: • $\mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[x]/(x^2+5)$ is a quotient of a Noetherian ring, hence it is Noetherian.

• $\mathbb{Z}[\sqrt{-5}]$ is not a PID, and it is not a UFD.
Also $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ are 2 distinct factorizations into irreducibles (Show: $N(2) = 4$, $N(3) = 9$, $N(1+\sqrt{-5}) = 6 \Rightarrow$ they are irreducible)

⚠ Subrings / Quotient rings of UFDs need not be UFDs.

Example 1: $\mathbb{Z}$ is a UFD (because it is a Euclidean domain), so $\mathbb{Z}[x]$ is also a UFD. Take $I = (x^2+5)$
Then $\mathbb{Z}[x]/I \cong \mathbb{Z}[\sqrt{-5}]$ is still a domain (quotient of domains are not necessarily domains) but it is not a UFD
$a + bx \pmod{I} \longleftrightarrow a + b\sqrt{-5}$
We saw this in Lectures 48 & 50 (. $\mathbb{Z}[\sqrt{-5}]$ is not a PID, hence not a UFD
. 3 is irreducible but not prime)

Example 2: $\mathbb{Z}[\sqrt{-5}] \subseteq \mathbb{C}$ is a subring. $\mathbb{C}$ is a field, hence a UFD, but $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Example 3: $R = \mathbb{Q}[x]$ is a UFD

$R_1 = \{ f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in \mathbb{Q}[x] \text{ s.t } a_1 = 0 \}$

$= \{ f(x) \in \mathbb{Q}[x] : f'(0) = 0 \} \subseteq R$

Claim 1: R_1 is a subring of R:

Pf/ • $0, 1 \in R$

• $f_1, f_2 \in R_1 \Rightarrow (f_1 \pm f_2)'(0) = f_1'(0) \pm f_2'(0) = 0 \pm 0 = 0$ so $f_1 \pm f_2 \in R_1$

• $f_1, f_2 \in R_1 \Rightarrow (f_1 f_2)'(0) = \underset{0}{f_1'(0)} f_2(0) + f_1(0) \underset{0}{f_2'(0)} = 0 + 0 = 0$, so $f_1 f_2 \in R_1$

Claim 2: R_1 is not a UFD.

Pf/ • $x^2 \in R_1$ is irreducible. Indeed, assume $x^2 = fg$ with $f, g \in R_1$. Then $\deg f = 0$ or $\deg g = 0$ (so f or $g \in \mathbb{Q} = R_1^\times$) or $\deg f = \deg g = 1$, but the latter cannot happen since $f_1, g_1 \in R_1$

• $x^2 \in R_1$ is not prime because $x^3 \cdot x^3 = x^6 \in (x^2)$ ($x^6 = x^2 x^4$ & $x^4 \in R_1$)

but $x^3 \notin (x^2) \subseteq R_1$ since $x^3 = x^2 x$ in R but $x \notin R_1$.

§55.2 Eisenstein's Criterion:

Next, we give another application of Gauss' Lemma

Theorem (Eisenstein Criterion for Irreducibility)

Let R be a UFD. Assume we have $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ with $\deg(f) = n \geq 1$. Let $p \in R$ be an irreducible element.

Assume: • $f(x)$ is primitive (ie gcd(coefficients of f) $= 1$)

• $a_n \not\equiv 0 \mod p$,

• $a_i \equiv 0 \mod p \quad \forall i \in \{0, \ldots, n-1\}$

• $a_i \not\equiv 0 \mod p^2$

Then, $f(x)$ is irreducible in $R[x]$

Remark: By Gauss's Lemma, this is equivalent to saying $f(x)$ is irreducible in $F[x]$ where F is the field of fractions of R.

Proof: Assume $f(x) = g(x)\,h(x)$ for some $g(x), h(x) \in R[x]$.

If $f(x)$ is not irreducible, then $g, h \notin R$ (Here we use the primitive condition)

Thus, we write $g(x) = b_k x^k + b_{k-1} x^{k-1} + \cdots + b_0$

$h(x) = c_\ell x^\ell + c_{\ell-1} x^{\ell-1} + \cdots + c_0$

with $k, \ell \geq 1$ and $k + \ell = n = \text{degree}(f(x))$

- As $b_0 c_0 = a_0 \equiv 0 \mod p$ we set that exactly one of b_0, c_0 is $\not\equiv 0 \mod p^2$

divisible by p. Without loss of generality, we assume $p \mid c_0$ & $p \nmid b_0$.

- On the other extreme: $a_n = b_k c_\ell \not\equiv 0 \mod p \Rightarrow p \nmid b_k$ & $p \nmid c_\ell$

We have $h(x) = c_\ell x^\ell + c_{\ell-1} x^{\ell-1} + \cdots + c_0 \Rightarrow \exists\ 1 \leq r \leq \ell < n$ such that

(c_ℓ: not divisible by p; c_0: divisible by p)

$c_0, \ldots, c_{r-1} \equiv 0 \mod p$ (ie $p \mid c_0, \ldots, p \mid c_{r-1}$)

$c_r \not\equiv 0 \mod p$ (ie $p \nmid c_r$)

Now, we look at the coefficient of x^r in $f(x)$:

$$a_r = \underbrace{b_0 c_r}_{p \nmid} + \underbrace{b_1 c_{r-1} + \cdots + b_r c_0}_{p \mid} \Rightarrow p \nmid a_r \quad \text{ie} \quad a_r \not\equiv 0 \pmod p$$

By our assumptions: $r = n$ Contradiction! □

§55.3 Examples:

① $f(x) = x^2 + 4x + 2 \in \mathbb{Z}[x]$ $(\subset \mathbb{Q}[x])$ is irreducible

Solution 1: $f(x) = (x+2)^2 - 2 = (x + 2 - \sqrt{2})(x + 2 + \sqrt{2})$

If for sake of a counterexample $f(x) = (x-\alpha)(x-\beta)$ for $\alpha, \beta \in \mathbb{Q}$

then $f(\alpha) = 0$ ie $\alpha = -2 \pm \sqrt{2} \in \mathbb{Q} \Rightarrow \sqrt{2} \in \mathbb{Q}$ Contradiction!

Solution 2: Take $p = 2$ in Eisenstein's Criterion.

$a_2 = 1 \not\equiv 0 \mod 2$, $a_1 = 4 \equiv 0 \mod 2$, $a_0 = 2 \not\equiv 0 \mod 4$

$a_0 = 2 \equiv 0 \mod 2$

② $f(x) = x^2+x+1 \in \mathbb{Z}[x]$ is irreducible

Solution 1: Over $\mathbb{C}$: $f(x) = \frac{x^3-1}{x-1} = (x-\omega)(x-\omega^2)$ where $\omega = \frac{-1\pm\sqrt{3}i}{2}$

If $f(x) = (x-\alpha)(x-\beta)$ for $\alpha, \beta \in \mathbb{Q}$, then $\alpha = \omega \in \mathbb{Q} \Rightarrow \sqrt{3}i \in \mathbb{Q}$ Contr!

Solution 2: Change $f(x)$ to $g(x) = f(x+1) =$

$$\begin{array}{r} x^2+2x+1 \\ +\quad\quad x+1 \\ \hline x^2+3x+3 \end{array}$$

Take $p=3$ in Eisenstein's Criterion to show $f(x+1)$ is irreducible

If $f(x)$ factors, so does $f(x+1)$ because $\forall h \in \mathbb{Q}[x]$ $\deg h(x) = \deg(h(x+1))$.