Lecture 50

(50.0) Recall: Let R be a commutative ring which in addition is an integral domain.

- A non-zero, non-unit element ($a \in R$) is said to be irreducible if, for $x, y \in R$, we have $a = x \cdot y$, then either x or y is a unit.
- R is a 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 $a \in R$; $a \neq 0$; $a \notin R^\times$, there exist irreducible elements $p_1, \dots, p_\ell \in R$ [not necessarily distinct] so that

$$a = p_1 \cdot p_2 \cdots p_\ell \qquad \text{(existence of factorization)}.$$

Moreover, if $a = q_1 q_2 \cdots q_k$ where $q_1, \dots, q_k \in R$ are also irreducible, then $k = \ell$, and there is a permutation σ of $\{1, \dots, \ell\}$; and units $u_1, \dots, u_\ell \in R^\times$ so that

$$q_i = u_i \, p_{\sigma(i)} \qquad \forall \; i \in \{1, \dots, \ell\}$$

(uniqueness of factorization).

(50.1) Basic facts about U.F.D.'s. Let R be a U.F.D.

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

(see Lemmas 49.0 and 49.1 from the previous lecture.)

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

and | greatest common divisor of coefficients of $p(x) = 1$ |.

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

$$p(x) = A(x) \cdot B(x) \quad \text{where } A(x), B(x) \in F[x]$$

(say, degrees of A and B are ≥ 1)

Then $$p(x) = a(x) \cdot b(x) \quad \text{where } a(x), b(x) \in R[x]$$

and $\text{degree}(a) = \text{degree}(A)$

$\text{degree}(b) = \text{degree}(B)$.

In fact, $a(x) = \lambda \cdot A(x)$ and (hence) $b(x) = \lambda^{-1} \cdot B(x)$

for some $\lambda \in F \setminus \{0\}$ $(= F^{\times})$.

[See page 9 of Lecture 49 – proof of Gauss' Lemma.]

(50.2) Consequence of Gauss' Lemma and the fact that

$K[x]$ is a unique factorization domain, for any field K

is the following:

$$R : \text{UFD} \implies R[x] \text{ is a U.F.D.}$$

- Subring / Quotient rings of U.F.D. NEED NOT BE U.F.D..

Example 1: $\mathbb{Z}$ is a unique factorization domain (being Euclidean domain (a)). Hence $\mathbb{Z}[x]$ is also a unique factorization domain. Take $I = (x^2+5)$.

[Ex.] $\mathbb{Z}[x]/I \cong \mathbb{Z}[\sqrt{-5}]$ still a domain, but not a U.F.D.

[of course, a quotient ring of a domain need not be a domain after all.]

Example 2: $R = \mathbb{Q}[x]$ is a U.F.D. (this works more generally for any field K.)

$$R_1 := \{ f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n \in \mathbb{Q}[x] \text{ such that } a_1 = 0 \}$$

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

($f'(x)$ ← derivative of $f(x)$; $\subset$ ← subring (check!))

Claim: R_1 is not a unique factorization domain.

Proof. (i) $x^2 \in R_1$ is an irreducible element (easy exercise.)

(ii) ~~$(x^3) \cdot (\quad)$~~ $x^3 \cdot x^3 \in (x^2)$ but $x^3 \notin (x^2)$

((x^2) ← ideal in R_1)

$\Rightarrow (x^2)$ is not a prime ideal.

Example 3.

$$\mathbb{Z}[\sqrt{-5}] \subset \mathbb{C}$$

($\subset$ ← subring; $\mathbb{Z}[\sqrt{-5}]$ ← not a U.F.D.; $\mathbb{C}$ ← field; hence U.F.D.)

(50.3) Another application of Gauss' Lemma:

Eisenstein Criterion for checking irreducibility of a polynomial.

Let R be a unique factorization domain. Assume we have $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in R[x]$, with $n = \text{degree}(f(x)) \geq 1$. ; and $p \in R$ an irreducible element.

Hypotheses :

- g.c.d. (coefficients of $f(x)$) $= 1$.
- $a_n \not\equiv 0 \pmod p$
  $a_i \equiv 0 \pmod p$ for every $i \in \{0, \dots, n-1\}$
  $a_0 \not\equiv 0 \pmod{p^2}$

Conclusion $f(x)$ is irreducible (in $R[x]$, or what is the same thing, in $F[x]$ — by Lemma 49.5 page 9 of lecture 49). (F = field of fractions of R)

Proof. Let us say $f(x) = g(x) \cdot h(x)$; for some $g(x), h(x) \in R[x]$

$$g(x) = b_k x^k + b_{k-1} x^{k-1} + \dots + b_1 x + b_0$$
$$h(x) = c_\ell x^\ell + c_{\ell-1} x^{\ell-1} + \dots + c_1(x) + c_0$$

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

- As $b_0 c_0 = a_0 \equiv 0 \pmod p$ and $\not\equiv 0 \pmod{p^2}$ } we get (that exactly) one of b_0, c_0 is divisible by p.

Say : $p \mid c_0$ and $p \nmid b_0$.

- On the other extreme $a_n = b_k c_\ell \not\equiv 0 \pmod p$

$\Rightarrow \quad p \nmid b_k \quad$ and $\quad p \nmid c_\ell$.

Thus, for $h(x) = c_\ell x^\ell + c_{\ell-1} x^{\ell-1} + \dots + c_1 x + c_0$

c_ℓ: not divisible by p.

c_0: divisible by p

There exists r so that

$$c_0, \dots, c_{r-1} \equiv 0 \pmod p$$

$$c_r \not\equiv 0 \pmod p$$

(thus $1 \le r \le \ell < n$ because $\ell = n-k$ & $k \ge 1$.)

Now

$$a_r = b_0 c_r + \boxed{b_1 c_{r-1} + \dots + b_r c_0}$$

$b_0 c_r$: not divisible by p

$\boxed{\dots}$: all divisible by p

$\Rightarrow \quad a_r \not\equiv 0 \pmod p$. Contradiction! $\square$

(50.4) e.g. $f(x) = x^2 + 4x + 2 \in \mathbb{Z}[x]$ is irreducible. (or $\mathbb{Q}[x]$)

Soln. 1 $f(x) = (x+2)^2 - 2$

$= (x+2-\sqrt{2})(x+2+\sqrt{2})$

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

then $f(\alpha) = 0$; i.e. $\alpha = -2 \pm \sqrt{2}$; i.e. $\sqrt{2} \in \mathbb{Q}$ contradiction.

Soln. 2 Take $p = 2$ in Eisenstein's criterion.

(50.5) Example. $f(x) = x^2 + x + 1$

Soln. 1 Over $\mathbb{C}$: $f(x) = \frac{x^3 - 1}{x - 1} = (x-\omega)(x-\omega^2)$

where $\omega = -\frac{1}{2} \pm \frac{\sqrt{3}}{2} i$. Same logic as before

Soln. 2 Change $f(x)$ to $g(x) = f(x+1)$

$= x^2 + 2x + 1$
$\quad + x + 1$
$\quad\quad + 1$

$x^2 + 3x + 3$

Take $p = 3$ in Eisenstein Criterion!