LECTURE 31

Dec. 3/2003.

R domain

R Euclidean ($\exists\, \delta : R - \{0\} \to \{+1, +2, \dots\}$ s.t. $\forall\, a, b \in R$, $\exists\, q, r \in R$ s.t. $b = qa + r$ & $r = 0$ or $\delta(r) < \delta(a)$)

$\boxed{\text{Examples } \mathbb{Z}, F[X], \mathbb{Z}[i]}$

$\Downarrow$

Every ideal $I \subset R$ is principal (i.e. $I = (d)$)

$\Downarrow$

Every element in R has a unique prime factorization ($a = u\, \underbrace{p_1 \cdots p_r}_{\text{primes, unique up to order.}}$), u unit

p in R is prime $\iff$ $(p) \subsetneq R$ is maximal wrt principal ideals.

$\iff$ $R/(p)$ is an integral domain

If $R/(p)$ is not a field, then $\exists\, I$ s.t. $(p) \subsetneq I \subsetneq R$, and so I is not principal.

Example: $R = \mathbb{Z}[X]$, $p = X$

$R/(X) \simeq \mathbb{Z}$ is a domain but not a field.

e.g. $I = (X, 2)$ is a non-principal ideal between (X) & R; $R/I \simeq \mathbb{Z}/(2)$

In fact: Even though $\mathbb{Z}[X]$ is not a principal ideal domain, it does have unique factorization. This follows from:

Proposition: In fact, if R is a domain with unique factorization into primes, so is $R[X]$.
(and so by induction $R[X_1, \dots, X_n]$ has unique factorization.)

Let's consider just what's happening in $\mathbb{Z}[X]$:

$f(x) \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$.

$\Vert$ ← can factor into primes of $\mathbb{Q}[X]$ since $\mathbb{Q}[X]$ is Euclidean $\Rightarrow$ unique fact. dom.

$\underset{\substack{\uparrow \\ \mathbb{Q}^\times}}{c} \cdot p_1(X) \cdots p_k(X)$

monic, irred. polys in $\mathbb{Q}[X]$.

Analog of monic in $\mathbb{Z}[X]$ is "primitive polynomial":

We say $f_0 = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$ is primitive if $\gcd(a_n, a_{n-1}, \dots, a_0) = 1$
(i.e. $\underset{\substack{\uparrow \\ \text{ideal gen'd by } a_0, \dots, a_n}}{(a_0, a_1, \dots, a_n)} = \mathbb{Z}$).

Artin also assumes as part of the def'n of primitive that $a_n > 0$.

<u>Rmk</u> Any $f \in \mathbb{Z}[X]$ can be written <u>uniquely</u> as $c \cdot f_0$ where $c \in \mathbb{Z}$ and f_0 is primitive in $\mathbb{Z}[X]$.

<u>Rmk</u> In fact, if $f(X) \in \mathbb{Q}[X]$, then $f(X) = c \cdot f_0(X)$ uniquely where $c \in \mathbb{Q}^\times$ and $f_0(X)$ is primitive in $\mathbb{Z}[X]$.
Moreover $f(X) \in \mathbb{Z}[X]$ to start with, if and only if $c \in \mathbb{Z}$.

<u>Def'n</u> This constant c above is called the "<u>content</u>" of $f(X)$.

Now let's return to our factorization of $f(X)$ in $\mathbb{Q}[X]$:

$$f(X) = c \cdot p_1(X) \cdots p_k(X).$$

Rewrite each $p_i(X)$ as $c_i q_i(X)$ where $c_i \in \mathbb{Q}^\times$ & $q_i(X)$ is a primitive poly in $\mathbb{Z}[X]$:

so $f(X) = d \, q_1(X) \cdots q_k(X)$.
(where $d = c \cdot c_1 \cdots c_k$)
& each $q_i(X)$ is irreducible in $\mathbb{Z}[X]$.

Gauss' Lemma If f_0 & g_0 are primitive polynomials in $\mathbb{Z}[X]$, so is $f_0 g_0$.

From this lemma:
it follows that $q_1 \cdots q_k$ is primitive & so its ~~content~~ $q_1 \cdots q_k$ is 1; moreover this shows the content of $f(X)$ is d; however $f(X) \in \mathbb{Z}[X]$ so by earlier remark $d \in \mathbb{Z}$.

Pf) (of Gauss' lemma)
Suppose it is not primitive, and say the prime p divides all coeffs of $f_0(X) g_0(X)$.
Consider the ring hom.

$$\mathbb{Z}[X] \longrightarrow \mathbb{Z}/p\mathbb{Z}[X]$$
$$a_0 + \cdots + a_n X^n \longmapsto \overline{a_0} + \cdots + \overline{a_n} X^n$$

Now $\mathbb{Z}/p\mathbb{Z}[X]$ is a domain.

Then $\overline{f_0(X)}\,\overline{g_0(X)} = 0$

So either $\overline{f_0(X)} = 0$ or $\overline{g_0(X)} = 0$, contradicting primitivity. $\boxtimes$

So now factor d into a product of primes of $\mathbb{Z}$: $\pm l_1 \cdots l_s$.

So we've written

$f(X) \in \mathbb{Z}$ as $f(X) = \pm l_1 \cdots l_s \; q_1(X) \cdots q_k(X)$

l_i are integer primes
& $q_i(X)$ are primitive
irreducible polys of $\mathbb{Z}[X]$

This is the unique factorization of $f(X)$ into primes in $\mathbb{Z}[X]$.

<u>Rmk</u> This method generalizes to prove that if R has unique factorization, $R[X]$ does too.

<u>Rmk</u> It's sometimes easier to prove that a poly in $\mathbb{Z}[X]$ is irreducible (than to prove irred. in $\mathbb{Q}[X]$) since you can check irreducibility easily in $\mathbb{Z}/p\mathbb{Z}[X]$ for primes p.
(if irred. in $\mathbb{Z}/p\mathbb{Z}[X]$ for some p then irred in <u>$\mathbb{Z}[X]$</u>.)

Example: $X^2+X+1 \in \mathbb{Z}[X]$ is irreducible.

Pf) Show that X^2+X+1 is irreducible in $\mathbb{Z}/2[X]$ (Follows e.g., because has no roots.) $\boxtimes$.

WARNING: There is no guarantee that this method will work to show irreducibility in $\mathbb{Z}[X]$.

There are polynomials in $\mathbb{Z}[X]$ which are irreducible, but reducible mod p for every prime p.