LECTURE 27

Nov. 19/2003.

Last time, relations $a_1 = a_2 = \cdots = a_n = 0$ in R

$$R \xrightarrow[f]{} \overline{R} = R/(a_1, \ldots, a_n)$$

$$(a_1, \ldots, a_n) = \{r_1 a_1 + \cdots + r_n a_n : r_i \in R\}.$$

Now we will treat adjoining elements α to a ring R

Ex:

$$\mathbb{Z} \subset R \subset R[\alpha] \subset \mathbb{C} \ni \alpha$$

$R[\alpha] = R' = \{$all polynomials $r_0 + r_1\alpha + r_2\alpha^2 + \cdots + r_n\alpha^n : r_i \in R, n \geq 0\}$

= the smallest subring of $\mathbb{C}$ containing both R and α

> NOTE: There's nothing special about $\mathbb{C}$; we're just using it as an example.

The structure of R' depends on α!
For example, if $\alpha \in R$, then $R' = R$
Here $\alpha \in R$ satisfies a monic poly $/R$:
$X - \alpha = 0$.

More generally: if α satisfies a monic polynomial of minimal degree n over R:
e.g. $X^2 + 1 = 0$ $(\Rightarrow \alpha = i)$
then $R' = \{r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1} : r_i \in R\}$
$(\simeq R^n$ as a group under $+)$

For example: $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$

However, it may be the case that α doesn't satisfy a monic poly$/_R$ but does satisfy some poly$/_R$ $\leftarrow$ this case is difficult to analyze.

Another possibility is that ~~that~~ α doesn't satisfy <u>any</u> polynomial with coeffs in R. Then we say α is <u>transcendental</u> over R

<u>Ex</u>: π is transcendental (π = area of circle of radius 1) over $\mathbb{Z}$ & $\mathbb{Q}$

Also: e = base of natural log is transcendental over $\mathbb{Z}$ & $\mathbb{Q}$.

Back in case where α satisfies monic poly $f(X)$ of minimal degree over R:

$$R[\alpha] \simeq R[X]/(f(X)).$$

Or put another way: — In complete generality: If we want a larger ring than R, containing a new element α satisfying a monic poly $f(X)$ over R, we can take the ring

$$R' = R[X]/(f(X))$$

(So, in particular, we don't need an ambient ring like $\mathbb{C}$)

Ex: $\mathbb{Z}[i] = \mathbb{Z}[X]/(X^2+1)$.

Ex: $R = \mathbb{Z}/(3) = \{0,1,2\}$ } Note that $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 1$ so: 2 is not a square in $\mathbb{Z}/3$;

$\rightarrow$ Put another way: $f(X) = X^2 - 2$ is irreducible in $\mathbb{Z}/3\mathbb{Z}$ as it has no roots & is quadratic.

[Def'n Irreducible means $f(X) \neq g(X)\,h(X)$ where $\deg g, \deg h \geq 1$]

Note: Can't test irreducibility by detecting roots for polys of degree ≥ 4.
But luckily we can for quadratic polys.

So consider $R' = (\mathbb{Z}/3\mathbb{Z}[X])/(X^2-2)$
$= \mathbb{Z}/3\mathbb{Z} + \mathbb{Z}/3\mathbb{Z}\cdot X \leftarrow$ 9 elements

Claim R' is a field

Pf $(a+bX)(a-bX) = a^2 - 2b^2 \neq 0$ in $\mathbb{Z}/3\mathbb{Z}$ if $a, b \neq 0$.

(This follows because if $a^2-2b^2=0$ with $b \neq 0$, then $a^2=2b^2 \Rightarrow (a/b)^2=2$ (contradiction))

Thus have $(a^2-2b^2)^{-1} \in \mathbb{Z}/3\mathbb{Z}$ exists & so $(a+bX)\left(\frac{a-bX}{a^2-2b^2}\right)=1$. ☒

More generally:
Let F be a field, let $f(X)$ be a monic polynomial w/ coeffs in F, degree n.
Consider the ring $R = F[X]/(f(X))$ ($\cong F^n$ as groups under $+$)

<u>Prop</u> R is a field $\Longleftrightarrow$ $f(X)$ is irreducible over F.

<u>NOTE ON THIS:</u> It <u>doesn't</u> mean that for any polys of same degree, f, g, $F[X]/(f(X))$ $F[X]/(g(X))$ are the same — they are <u>not</u> in general isomorphic as fields!

<u>Pf of prop'n</u>).
R is a field $\Longleftrightarrow$ the only ideals are 0 & R
$\Longleftrightarrow$ there are exactly 2 ideals in $F[X]$ containing $I=(f(X))$, namely I & $F[X]$.
$\Longleftrightarrow$ $(f(X))$ is a max'l ideal of $F[X]$

<u>But</u> we know the ideals of I in $F[X]$.
They are all of the form $(g(X))$.

and we know $(f(X)) \subset (g(X)) \subset F[X]$
if & only if $g(X)$ divides $f(X)$.
Thus $(f(X))$ is maximal
$\Leftrightarrow$ there is no polynomial of smaller degree dividing $f(X)$
$\Leftrightarrow$ $f(X)$ is irreducible.
Conclusion: R is a field $\Leftrightarrow$ $f(X)$ is irred.
$\boxtimes$

<u>Ex</u>: To produce a field F' of order p^2, we need an <u>irreducible</u> quadratic polynomial $\overline{X^2+bX+c}$ over $\mathbb{Z}/p\mathbb{Z}$..

$p=2$: $f(X) = X^2+X+1$ is irred.
(since has no roots & is quadratic)

$\mathbb{F}_4$ = field with 4 elements
$= (\mathbb{Z}/2[X]) / (X^2+X+1)$.

$p>2$: $f(X) = X^2 - c$ will be irred.
if <u>c is not a square in $\mathbb{Z}/p\mathbb{Z}$</u>.

To find such a c:
consider $(\mathbb{Z}/p\mathbb{Z})^\times \xrightarrow[h]{} (\mathbb{Z}/p\mathbb{Z})^\times$
(ab. gp. of order $p-1$) $\quad h(a) = a^2$.
h is a gp. hom.

The claim that we can find a non-square is the claim that h is <u>not surjective</u> (since the image is exactly the set of squares)

Since the domain of h has the same order as the target, h is not surjective if and only if h is <u>not injective</u>, which is true if and only if h has nontrivial kernel.

$\ker h \ni -1$ so kernel is nontrivial, as desired.

(In fact $|\mathrm{Image}(h)| = \frac{p-1}{2}$ since $\ker h = \{\pm 1\}$).

So take any c not in the image of h &

$(\mathbb{Z}/p)[X]) / (X^2 - c)$ is field of order p^2.

//