LECTURE 26 Nov. 17/2003

R commutative ring

Have canonical map
$f: \mathbb{Z} \to R$ ring hom.
characterized by $f(1) = 1_R$
For $n \geq 1$: $f(n) = f(\underbrace{1 + \cdots + 1}_{n \text{ times}}) = \underbrace{1_R + \cdots + 1_R}_{n \text{ times}}$
$f(-n) = -f(n)$.

$\ker(f)$ is an ideal of $\mathbb{Z}$ & hence is of the form $n\mathbb{Z}$ $(n \geq 0)$

Ex.: If $R = \{0\}$, $\ker f = \mathbb{Z}$
If $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, $\ker f = 0 \cdot \mathbb{Z} = \{0\}$
If $R = \mathbb{Z}/n\mathbb{Z}$, then $\ker f = n\mathbb{Z}$

Prop If R is a field, $\ker f = \begin{cases} (0) \\ p\mathbb{Z} & \text{for } p \text{ a prime number} \end{cases}$

Pf) Suppose $\ker f = n\mathbb{Z}$,
where n is composite, say
$n = a \cdot b$ $(a > 1, b > 1)$
Then in R, $0_R = f(n) = f(a) \cdot f(b)$
$= a_R \cdot b_R$
If $a_R \neq 0$, multiply by a_R^{-1} to get $b_R = 0$. So one of a_R, b_R must be 0. So $a \in \ker f$ or $b \in \ker f$.
Contradiction, since $a, b \notin n\mathbb{Z}$. $\boxtimes$

Notation If as above $\ker f = (0)$, we say the field R has characteristic 0 & if $\ker f = (p)$, we say the field R has characteristic $p > 0$.

Thm (Galois)
Let F be a finite field.
Then $|F| = p^f$ for some prime p.

Pf) Consider the canonical map

$$\mathbb{Z} \longrightarrow F$$
$$n \longmapsto n_F$$

Since F is finite, this can't be an injection, so $\ker f \neq (0)$.
So $\ker f = (p)$, and f induces a ring homomorphism:

1st Isomorphism Theorem for Rings

$$\bar{f} : \mathbb{Z}/p\mathbb{Z} \hookrightarrow F$$

This gives F the structure of a vectorspace over the field $\mathbb{Z}/p\mathbb{Z}$, which has finite dimension (since F is itself finite), say dim'n f.
Therefore $|F| = p^f$. $\boxtimes$.

Note: We will show later that for every $f \geq 1$, and prime p, there is a unique field F with $|F| = p^f$.
We need some additional theory to do this, though.

Quotient rings & Isomorphism thms

$R \supset I$ ideal

$R \xrightarrow{f} R/I = \overline{R}$ quotient ring

surjective ring hom.

Prop There is a bijection

$$\left\{ \begin{array}{c} \text{ideals } I \subset J \subset R \\ \text{of } R \text{ containing } I \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{ideals } \overline{J} \\ \text{of } \overline{R} \end{array} \right\}$$

$$J \longmapsto f(J) \subset \overline{R}$$

$$f^{-1}(\overline{J}) \longleftarrow \overline{J}$$

Moreover $R/J \simeq \overline{R}/\overline{J}$, isomorphism of quotient rings.

Pf) Easily verify:

- Given ideal J of R containing I, $f(J)$ is an ideal of $\overline{R}$ (need to use surjectivity of $R \to R/I$)
- Likewise, given ideal $\overline{J}$ of $\overline{R}$, it's easy to verify $f^{-1}(\overline{J})$ is ideal of R & it contains I.
- $f(f^{-1}(\overline{J})) = \overline{J}$ & $f^{-1}(f(J)) = J$ again by given hypotheses

• remains to check
$R/J \simeq \bar{R}/\bar{J}$
this follows from usual first isomorphism thm for rings
$R \longrightarrow \bar{R}/\bar{J}$ is surjective
with kernel $J = f^{-1}(\bar{J})$
so $R/J \simeq \bar{R}/\bar{J}$.

$\boxtimes$

<u>Question</u>: When is R/I a field?

<u>Answer</u>: $\Leftrightarrow$ $\bar{R} = R/I$ has only two ideals: (0) & R
$\Leftrightarrow$ R has only two ideals containing I, namely I & R.

<u>Def'n</u> If $I \subset R$, $I \neq R$
we say I is <u>maximal</u> if there is no J containing I & ideal of R, other than I and R.

<u>Note:</u> The above shows:
R/I is a field $\Longleftrightarrow$ I is a <u>maximal ideal</u>.

Creating relations in a ring R

$a \in R$.

If we want a ring $\overline{R}$ which is an image of R, where $\overline{a} = 0$, then the largest such quotient is $\overline{R} = R/(a)$

If we want one where $a_1 = a_2 = \cdots = a_n = 0$ $(\Rightarrow r_1 a_1 + \cdots + r_n a_n = 0)$
take $\overline{R} = R/(a_1, a_2, \ldots, a_n)$

<u>Note:</u> could also construct this $\overline{R}$ as $R/(a_1)/(\overline{a_2})/(\overline{a_3}) \cdots$

- Let's make this concrete by considering what happens in the setting of $R = \mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i = \{a + bi : a, b \in \mathbb{Z}\}$.

<u>Ex:</u> Suppose we want "$2+i=0$".
Let $I = (2+i)$, $\overline{R} := R/I$.
Identify $\overline{R}$.
First, let's identify $I \cap \mathbb{Z}$.

<u>Claim 1</u> $5 \in I \cap \mathbb{Z}$.
Pf) $5 = (2+i)(2-i)$ $\boxtimes$
Hence $5\mathbb{Z} \subset I \cap \mathbb{Z}$
But 5 is prime, so can't fit any ideals strictly between $5\mathbb{Z}$ & $I \cap \mathbb{Z}$
So $I \cap \mathbb{Z}$ is either $\mathbb{Z}$ or $5\mathbb{Z}$.

<u>Claim 2</u> If $(2+i)(a+bi) \in \mathbb{Z}$ then it is in $5\mathbb{Z}$

<u>Pf)</u> $(2a-b)+(2b+a)i \in \mathbb{Z} \Rightarrow 2b+a=0$
$\Rightarrow a=-2b \quad \Rightarrow 2a-b=-4b-b=-5b.$ $\boxtimes$

Therefore $I \cap \mathbb{Z} = 5\mathbb{Z}$

Canonical map $\mathbb{Z} \to R/I = \overline{R}$ has kernel $5\mathbb{Z}$ and image $\mathbb{Z}/5\mathbb{Z}$.

In fact $\overline{R} \cong \mathbb{Z}/5\mathbb{Z}$ under this map.

Put another way: $\mathbb{Z} \to R/I$ is surjective.

Why is surjective?

Well: $i \equiv -2 \mod I$

So $bi \equiv -2b \mod I$.

So $a+bi \equiv \underbrace{a-2b}_{\in \mathbb{Z}} \mod I$. $\boxtimes$

Therefore $\underline{\underline{\overline{R} \simeq \mathbb{Z}/5\mathbb{Z}}}$.

<u>Theorem</u>

- More generally, if p is a prime number with $p \equiv 1 \pmod 4$ $\quad (p=5, 13, 17, 29, \ldots)$ then there is an ideal $I \subset \mathbb{Z}[i] = R$ with $R/I \simeq \mathbb{Z}/p\mathbb{Z}$.

<u>Pf)</u> Let $f: R \to R/I$ be the can. map.
If $f(i)$ has order 4 in $(\mathbb{Z}/p\mathbb{Z})^\times$ ($\leftarrow$ order $p-1$)
then $p \equiv 1 \pmod 4$

Note $(p-1)! \equiv -1 \pmod p$

(Wilson's theorem): it follows because can pair off elements & their inverses & left with -1)

It follows that $\left(\frac{p-1}{2}\right)!$ has (by same argument) order 4 mod p. This is our candidate for $f(i)$. Let $\underline{a = \left(\frac{p-1}{2}\right)!}$

Let I be the ideal generated by p & $i-a$.

(Notationally: $I = (p, i-a)$.

This actually works!

<u>Check</u>: $I \cap \mathbb{Z} = p\mathbb{Z}$

<u>Pf</u>) Clearly $p\mathbb{Z} \subset I \cap \mathbb{Z}$ since $p \in I$.

Also $(i-a)(b+ci) = (-ab-c) + (-ac+b)i$

& use $-ac+b=0$ to show $(i-a)(b+ci) \in p\mathbb{Z}$.

So indeed $I \cap \mathbb{Z} = p\mathbb{Z}$. $\boxtimes$.

Hence by same argument as in earlier example,

$$R/I \simeq \mathbb{Z}/p\mathbb{Z}. \qquad \boxtimes.$$

But <u>Thm (Gauss)</u> Every $I \subset R$ is <u>principal</u>.

Since every I is principal, the one above is, in particular, $I = (x+iy)$, $R/I \simeq \mathbb{Z}/p\mathbb{Z}$. It follows that $x^2 + y^2 = p$. (In fact $|\mathbb{Z}[i]/(a+bi)| = a^2+b^2$ $(a, b \ne 0)$)