Field $\mathbb{F}$ → at most n n-th roots of unity

Quiz Example of comm ring R which has more than n n-th roots unity, some n.

Solutions $\mathbb{Z}/8$ $\{1,3,5,7\}$ $R_1 \times R_2$ $\{\pm 1\} \times \{\pm 1\}$ 2nd roots of unity.

Fields - rigid structures; Rings - much more flexibility.

$\mathbb{Z}/n$ field iff n is prime. General n?

Thm If $(n,m)=1$ $\mathbb{Z}/nm \simeq \mathbb{Z}/n \times \mathbb{Z}/m$

Proof $\exists a,b$ $an+bm=1 \pmod{nm}$

let

$e=an$. then

$e^2 = e \cdot e = an \cdot an \overset{\text{mod } nm}{=} an(1-bm) =$

$= an - abnm = an \pmod{nm}$ $= e$

$(bm)^2 = bm \pmod{nm}$

$R=\mathbb{Z}/nm$. what is $Re = Ran$

$(a,m)=1 \Rightarrow ac=1 \bmod m$ some c

If $e \subset R$ idempotent in comm. ring $e^2=e$

Re - ring, e is identity

$aebe = abe$ (use commutativity

$1-e$ complementary idempotent

$R(1-e)$ ring, $1-e$ is identity

Inclusion $Re \subset R$ is not unital

$e \mapsto e$, not 1.

id

(subring in a weak sense)

Prop:

$R \simeq Re \times R(1-e)$

$a = ae + a(1-e)$ unique presentation

$can \in Ran$, $can = n$. $\Rightarrow$ $Ran = Rn = \mathbb{Z}n \overset{\simeq \mathbb{Z}/m}{}$ in $\mathbb{Z}/nm$

all multiples of n

$\{0, 1, 2, \ldots\}$ isom of rings.

$\{0, n, 2n, 3n, \ldots an, \ldots (m-1)n\} \simeq \mathbb{Z}/m$ as ring

idempotent "in the middle"

naive isomorphism is only that of abelian groups

$\{0, 1, 2, 3, \ldots, m-1\}$

bm - complementary idempotent

$\mathbb{Z}/m \subset \mathbb{Z}/nm$ is "subring" in weak sense

$1 \longmapsto an$

$\mathbb{Z}/n \longrightarrow \mathbb{Z}/nm$

$1 \longmapsto bm$

Example: $13 \cdot 5 = 65 \quad n = 13,\ m = 5$

$a \cdot 13 + b \cdot 5 = 1 \qquad a = 2,\ b = -5 \qquad 26 - 25 = 1$

idempotents $26,\ -25$.

$$26^2 = 26 \cdot (1 + 25) = 26 + 26 \cdot 25 = 26 + 2 \cdot \underbrace{13 \cdot 5}\cdot 5 = 26 \ (\mathrm{mod}\ 65).$$

$$\begin{array}{ccc} \mathbb{Z}/5 & \to & \mathbb{Z}/65 \\ 1 & \mapsto & 26 \\ k & \mapsto & 26k \end{array} \qquad \text{non-unital inclusion} \qquad \begin{array}{ccc} \mathbb{Z}/13 & \to & \mathbb{Z}/65 \\ 1 & \mapsto & -5 \\ k & \mapsto & -5k. \end{array}$$

$$\begin{array}{ccc} \mathbb{Z}/n & \to & \mathbb{Z}/nm \\ 1 & \mapsto & an \\ k & \mapsto & kan \end{array},\ k \in \mathbb{Z}/n \qquad 1 = an + bm \qquad \begin{array}{ccc} \mathbb{Z}/m & \to & \mathbb{Z}/nm \\ 1 & \mapsto & bm \\ l & \mapsto & lbm \end{array},\ l \in \mathbb{Z}/m$$

Projection maps $\mathbb{Z}/nm \to \mathbb{Z}/n$ easy.

$$1 \longrightarrow 1$$

$$\begin{tikzcd} & \mathbb{Z}/nm \arrow[dl] \arrow[dr] & \\ \mathbb{Z}/n \arrow[ur, dashed, bend left] & \text{easy} & \mathbb{Z}/m \arrow[ul, dashed, bend right] \end{tikzcd}$$

$\uparrow$ harder to construct

Thm $n = p_1^{r_1} \cdots p_k^{r_k}$ prime decomposition

$$\Rightarrow \mathbb{Z}/n \cong \mathbb{Z}/(p_1^{r_1}) \times \mathbb{Z}/(p_2^{r_2}) \times \cdots \times \mathbb{Z}/(p_k^{r_k}).$$

Prop 1) $\mathbb{Z}/p^r$ a field iff $r = 1$.

2) (p) is the unique maximal ideal of $\mathbb{Z}/p^r$.

$$(\mathbb{Z}/p^r)^* = \{1 \le a \le p^r - 1 \mid (a, p^r) = 1,\} \Leftrightarrow (a,p) = 1.$$

$b \in (\mathbb{Z}/p^r)^* \Longleftrightarrow a$ not divisible by p. All non-invertible elements constitute a single maximal ideal. $(p) \subset \mathbb{Z}/p^r$ unique max ideal, unique prime ideal.

Exercise: find algorithm to construct inverse of $b \in (\mathbb{Z}/p^r)^*$.

Same approach works with polynomials $F[x]$

$(f(x), g(x)) = 1 \Rightarrow a(x)f(x) + b(x)g(x) = 1.$

$R = F[x]/(f(x)g(x))$ $\quad af$ - idempotent $\quad F[x]/(g(x)) \longrightarrow F[x]/(fg)$

$1 \longmapsto af$

$h \longmapsto ahf.$

<u>Thm</u> $F[x]/(f(x)g(x)) \simeq F[x]/(f(x)) \times F[x]/(g(x))$ if $(f,g)=1$.

$I_1, I_2 \subset R$ ideal $\quad$ coprime or comaximal if $I_1 + I_2 = R \Leftrightarrow$

$1 \in I_1 + I_2$

$1 = a + b, \; a \in I_1, b \in I_2$

<u>Thm</u> For coprime I_1, I_2 $\quad I_1 I_2 = I_1 \cap I_2$

$\forall$ ideals I, J

$I \cap J \supset IJ$

$R/I_1 I_2 \longrightarrow R/I_1 \times R/I_2$

$R \xrightarrow{\varphi} R/I_1 \times R/I_2 \quad \ker\varphi = I_1 \cap I_2$

$1 = x + y \quad x \in I_1, y \in I_2 \quad \varphi(x) = (0,1), \varphi(y) = (1,0). \Rightarrow \varphi$ is surjective. $\quad \phi(r_1 x + r_2 y) = (r_2, r_1)$.

$r_2 +$

$R/I_1 \cap I_2 \longrightarrow R/I_1 \times R/I_2$

Example

$\mathbb{Z}/(nm) \longrightarrow \mathbb{Z}/n \times \mathbb{Z}/m$ $\quad I_1 = (n), I_2 = (m)$

n, m - coprime