Mar 13

1. Fermat's small thm

2. R is a ring. u is a unit in R, then $(u)=R$.

3. Example 11.3.7 (b)(c)

1. Fermat's small thm: Given a prime number p, $\forall a \in \mathbb{Z}$, $a^p \equiv a \pmod p$

Pf: Consider $\mathbb{F}_p$, finite field with order p. $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

$a^p = a$ in $\mathbb{F}_p$

If $a=0$, in $\mathbb{F}_p$ $0^p = 0$ holds trivially.

We consider the case $a \neq 0$. $\Rightarrow$ a is invertible

$$a^p = a \iff a^{p-1} = 1$$

$\mathbb{F}_p^\times = \{x \in \mathbb{F}_p \mid x \neq 0\}$. is a multiplicative group of order $p-1$.

Since $a \in \mathbb{F}_p^\times$, $|\mathbb{F}_p^\times| = p-1$. $\Rightarrow$ $a^{p-1} = 1$ in $\mathbb{F}_p$.
$\Rightarrow$ $a^{p-1} \equiv 1 \pmod p$.
$a^p \equiv a \pmod p$

$\blacksquare$

2. R is a ring, u is a unit in R. then the principal ideal (u) generated by u is R.

Pf: $(u) = \{ux \mid x \in R\}$

Since R is a ring, it is closed under multiplication.

$\Rightarrow$ $(u) \subseteq R$

To check: $R \subseteq (u)$

Since u is a unit, denote its inverse by t, i.e. $ut = tu = 1$.

For $\forall x \in R$. $x = x \cdot 1 = x \cdot tu = (xt)u$
$x = 1 \cdot x = ut \cdot x = u(tx)$ $\Rightarrow$ $R \subseteq (u)$

We can conclude that $R = (u)$.

$\blacksquare$

left-ideal / right ideal
Ru, uR, RuR $\leftarrow$ two-sided ideal.

Example 11.5.7 How to add a root of an equation to a known ring/field.

(b) Let R' be obtained by adding an element δ to $\mathbb{F}_5$ with the relation $\delta^2 - 3 = 0$ (δ is the "root" of 3)

$$\mathbb{F}_5 = \begin{matrix} \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4} \\ \bar{0}, \bar{1}, \bar{4}, \bar{4}, \bar{1} \end{matrix} \Bigg\} \Rightarrow$$ There is no root of 3 in $\mathbb{F}_5$, so we need to add it.

$R' = \mathbb{F}_5[x] / (x^2 - 3)$ ← polynomial ring in one variable with coefficients in $\mathbb{F}_5$

$= \mathbb{F}_5[\delta] \qquad \delta = \bar{x}$

$$\underline{\delta^2} = (\bar{x})^2 = \overline{x^2} = \overline{x^2 - 3 + 3} = \overline{x^2 - 3} + \underline{\bar{3}}$$

$\overline{x^2-3} = \bar{0}$ in $\mathbb{F}_5[\delta]$

$\rightsquigarrow \delta^2 = 3$.

Elements in $\underline{R'}$ are of the form $\underline{a + b\delta}$, where $a, b \in \mathbb{F}_5$.

Generally, an element in R' is a polynomial in δ.

$$f(\delta) = a_0\delta^n + \cdots + a_{n-1}\delta + a_n, \quad a_0 \neq 0$$

Quotient $f(x)$ by $x^2 - 3$. $\Rightarrow$ $\underline{f(x) = p(x)(x^2-3) + r(x)}$

$$\deg r(x) < \deg (x^2 - 3) = 2$$

$\Rightarrow$ $r(x)$ is of deg 1, or it's a constant, or zero.

$$f(\delta) = p(\delta)(\delta^2 - 3) + r(\delta) \xrightarrow{\delta^2 - 3 = 0} f(\delta) = r(\delta) = a + b\delta$$

5 values, 5 values $\Downarrow$ $|R'| = 5 \times 5 = 25$

R' is a 2-dim vector space over $\mathbb{F}_5$.

$|R'| = 25$

Now we show that R' is a field.

Given $\underset{\neq 0}{\underline{a + b\delta}}$ in R', $(a + b\delta)(a - b\delta) = a^2 - (b\delta)^2 = a^2 - 3b^2 = c$

$c = 0$ if and only if $a = b = 0$. If a, b are nonzero

$$a^2 = 3b^2 \Leftrightarrow \left(\frac{a}{b}\right)^2 = 3, \quad \text{but } \frac{a}{b} \in \mathbb{F}_5 \quad \nrightarrow$$

$\Rightarrow$ If $c = 0$, then a, b are both zero.

If $a + b\delta \neq 0$, then $\underset{\text{in } \mathbb{F}_5}{c \neq 0}$. $\quad a + b\delta \cdot \frac{a - b\delta}{c} = 1$. $\Rightarrow (a + b\delta)^{-1} = \frac{a - b\delta}{c}$.

(c) What happens if the above steps applied to $\mathbb{F}_{11}$

$S = \mathbb{F}_{11}[x]/(x^2-3)$ $\quad$ $\mathbb{F}_{11}$ has roots of 3 already. $(\pm 5)^2 = 25 \equiv 3.$

$= \mathbb{F}_{11}[\delta]$. ← This is not a field.

$\underbrace{\delta-5}_{\neq 0}, \ \underbrace{\delta+5}_{\neq 0}.$ $\quad$ $(\delta-5)(\delta+5) = \delta^2-3 = 0$ in $\mathbb{F}_{11}$

Since their product is zero, they can't be invertible.