2/13/2019
(27)

## §11.8 Maximal ideals

When we adjoined a root to $\mathbb{F}_2$ for the quadratic $x^2+x+1 \in \mathbb{F}_2[x]$ that had no roots to create $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$

$= \{0, 1, \alpha, \alpha+1\}$ where $\alpha = \bar{x}$

was it luck that the result was again a field?

No! – $I \subset \mathbb{F}_2[x]$ ($= (x^2+x+1)$) was a maximal ideal, and it was maximal because $x^2+x+1$ was irreducible in $\mathbb{F}_2[x]$ ...

DEF'N: An ideal $M \subset R$ a ring is a maximal ideal if there are no ideals $I$ with $M \subsetneq I \subsetneq R$ ($= (1)$) ← called the unit ideal

PROP (11.8.2):

(i) A ring $R$ is a field $\Leftrightarrow$ $R$ has only 2 ideals, $\{0\} = (0)$, $R = (1)$

$\Leftrightarrow$ $(0)$ is a maximal ideal of $R$

(ii) An ideal $I \subset R$ a ring is maximal $\Leftrightarrow$ $R/I$ is a field

(iii) A ring homom. $R \xrightarrow{\varphi} R'$ has $\operatorname{im}(\varphi)$ a field $\Leftrightarrow$ $\ker(\varphi)$ is a maximal ideal of $R$

proof: For (i), note that $r \in R$ is a unit $\Leftrightarrow \exists\, s \in R$ with $sr = 1$

$\Leftrightarrow$ $(r) \ni 1$

$\Leftrightarrow$ $(r) = (1) = R$

so $R$ is a field $\Leftrightarrow$ every $r \in R - \{0\}$ is a unit

$\Leftrightarrow$ every $r \in R - \{0\}$ has $(r) = R$

$\Leftrightarrow$ every nonzero ideal $I$ in $R$ has $I = R$

$\Leftrightarrow$ $\nexists$ ideal $I$ with $(0) \subsetneq I \subsetneq R$

$\Leftrightarrow$ $(0)$ is a maximal ideal in $R$

For (ii), we should go back a note this easy fact...

CORRESPONDENCE THEOREM (11.4.3): One has a bijection for any ideal $I \subset R$ a ring

$$\{\text{ideals } \bar{J} \text{ of } R/I\} \longleftrightarrow \{\text{ideals } J \text{ with } I \subseteq J \subseteq R\}$$

$$\bar{J} := \{j+I : j \in J\} \longleftarrow\!\shortmid\; J$$

$$\bar{J} \longmapsto \bigcup_{j+I \in \bar{J}} (j+I)$$

proof: Same as for the additive group structures, it just proves itself! ∎

Knowing this, then $R/I$ is a field $\Leftrightarrow$ $R/I$ has $(\bar{0})$ a maximal ideal

$\Leftrightarrow \nexists\, \bar{J}$ an ideal of $R/I$ with $(\bar{0}) \subsetneq \bar{J} \subsetneq R/I$

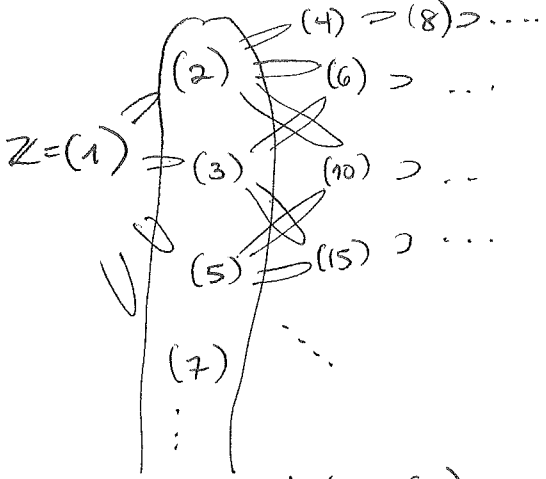
$\Leftrightarrow \nexists\, J$ an ideal of $R$ with $I \subsetneq J \subsetneq R$

$\Leftrightarrow$ $I$ is a max. ideal of $R$.

For (iii), note $R \xrightarrow{\varphi} R'$ has $\mathrm{im}(\varphi) \cong R/\ker(\varphi)$, so $\mathrm{im}(\varphi)$ a field $\Leftrightarrow$ $\ker(\varphi)$ maximal ∎

EXAMPLES ① $R = \mathbb{Z}$ has only principal ideals $I = (n)$,

and $(n) \subset (m) \Leftrightarrow m$ divides $n$, so the picture is this:




maximal ideals $= (p)$, $p$ prime $\Leftrightarrow \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ a field

② $R = \mathbb{F}[x]$ for $\mathbb{F}$ a field

also has only principal ideals $I = (f(x))$ (monic nonzero polynomial of least degree in $I$)

with $(g(x)) \subseteq (f(x)) \iff f$ divides $g$ in $\mathbb{F}[x]$

$\iff g(x) \in (f(x)) \iff g(x) = f(x)q(x)$

(so $(g(x)) = (f(x)) \iff g(x) = cf(x)$ for some $c \in \mathbb{F}^\times$).

Hence $M = (g(x))$ is maximal as an ideal

$\iff \nexists\ f(x)$ with $(1) \subsetneq (f(x)) \subsetneq (g(x))$

$\iff \nexists\ f(x)$ dividing $g(x)$ with $0 < \deg(f) < \deg(g)$,

DEFIN: $g(x)$ is irreducible in $\mathbb{F}[x]$ if this holds

---

e.g. $x^2+x+1 \in \mathbb{F}_2[x]$ is irreducible (Why?)

so $(x^2+x+1)$ is a maximal ideal in $\mathbb{F}_2[x]$

and $\mathbb{F}_2[x]/(x^2+x+1)$ is a field.

$\parallel$

$\mathbb{F}_4$

---

e.g. $x^2+1 \in \mathbb{R}[x]$ is irreducible (Why?)

so $(x^2+1)$ is a maximal ideal in $\mathbb{R}[x]$

and $\mathbb{R}[x]/(x^2+1)$ is a field.

$\parallel$

$\mathbb{C}$

---

e.g. $x^2+1 \in \mathbb{C}[x]$ is not irreducible, since $x^2+1 = (x+i)(x-i)$

so $(x^2+1)$ is not a maximal ideal

$\Rightarrow \mathbb{C}[x] \supsetneq \begin{matrix}(x+i)\\(x-i)\end{matrix} \supsetneq (x^2+1)$

$\mathbb{C}[x] = (1)$

and $\mathbb{C}[x]/(x^2+1)$ is not a field,

e.g. $\bar{x}+i \neq \bar{0}$ but $(\bar{x}-i)(\bar{x}+i) = \bar{0}$.

↑ both maximal ideals in $\mathbb{C}[x]$

(30)

(3) $x^2+1$ is irreducible in $\mathbb{F}_3[x]$ (why?)

and $x^3+x+1$ is irreducible in $\mathbb{F}_2[x]$ (why?)

Hence $\mathbb{F}_3[x]/(x^2+1)$ is a field with $9 = 3^2$ elements ($\cong \mathbb{F}_3^2$ as $\mathbb{F}_3$-vector space)

$$=: \mathbb{F}_9 = \{0, 1, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}$$

($\alpha = \bar{x}$, $\boxed{\alpha^2 = -1}$)

and $\mathbb{F}_2[x]/(x^3+x+1)$ is a field with $8 = 2^3$ elements

$$=: \mathbb{F}_8 = \{0, 1, \beta, \beta+1, \beta^2, \beta^2+1, \beta^2+\beta, \beta^2+\beta+1\}$$

($\beta = \bar{x}$, $\boxed{\beta^3 = \beta+1}$)

(We'll see later that (i) there is an irreducible $f(x)$ of degree $d$ in $\mathbb{F}_p[x]$ for every $d \geq 1$, letting us create $\mathbb{F}_{p^d}$

(ii) any two such $\mathbb{F}_{p^d}$ are isomorphic as rings)