(19)

proof: Same as for why $\overset{R}{\mathbb{Z}}/\overset{I}{n\mathbb{Z}}$ was a ring;

check $\times$ is well-defined, i.e. if $a+I=a'+I$ i.e. $a'=a+i_1$
$b+I=b'+I$ $b'=b+i_2$ with $i_1,i_2\in I$

then $(a'+I)(b'+I) \overset{?}{=} (a+I)(b+I)$

$(a'+I)(b'+I) = a'b'+I$

$= (a+i_1)(b+i_2)+I$

$= ab + \underbrace{ai_2}_{\in I} + \underbrace{bi_1}_{\in I} + \underbrace{i_1 i_2}_{\in I} + I$

$\underbrace{\qquad\qquad}_{\in I}$

$= ab+I$ ✓ $(a+I)(b+I) = ab+I$

The rest is all easy. ∎

EXAMPLES: (1) Since every ideal $I \subset \mathbb{Z}$ is $I = \overset{=(n)}{n\mathbb{Z}}$ (principal) for some n (maybe $n=0$)

every quotient ring of $\mathbb{Z}$ is either $\mathbb{Z}/n\mathbb{Z}$
or $\mathbb{Z}/\{0\} = \mathbb{Z}$ itself.

(2) Something similar happens for $\mathbb{F}[x]$, $\mathbb{F}$ a field...

PROP (11.3.22 / 11.5.5) (a) Every nonzero ideal $I \subset \mathbb{F}[x]$ for a field $\mathbb{F}$
is principal, $I = (f(x))$
generated by any nonzero monic polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$
of lowest degree in I.

(b) In this case, the quotient ring $\mathbb{F}[x]/(f(x)) = \mathbb{F}[x]/I$
is isomorphic as an $\mathbb{F}$-vector space to $\mathbb{F}^n$,
with $\mathbb{F}$-basis $\{1, a, a^2, \dots, a^{n-1}\}$ where $a = x+I = \bar{x}$ in $\mathbb{F}[x]/I$

2/8/2019
(20)

proof: (a) Given an ideal $I \subset \mathbb{F}[x]$ with $I \neq \{0\}$,

pick $f(x) \neq 0$ monic of smallest degree in I.

Certainly $f(x) \in I \Rightarrow (f(x)) \subseteq I$,

but conversely, given $g(x) \in I$ one can write

$$\underbrace{g(x)}_{\in I} = \underbrace{f(x)}_{\in I} \cdot g(x) + \underbrace{r(x)}_{\deg(r) < \deg(f)} \quad \underbrace{\in I}_{\in I}$$

$$\Rightarrow r(x) = g(x) - f(x)g(x) \in I$$

$$\Rightarrow r(x) = 0 \text{ since } \deg(r) < \deg(f)$$

$$\Rightarrow g(x) \in (f(x))$$

Thus $I = (f(x))$.

(b) Rephrased, this is saying that the map

$$\mathbb{F}^n \xrightarrow{\varphi} \mathbb{F}[x]/\overbrace{(f(x))}^{I}$$

$$\underline{a} = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} \longmapsto a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_{n-1}\alpha^{n-1}$$

$$= a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + I$$

is an $\mathbb{F}$-vector space isomorphism;

i.e. It is $\mathbb{F}$-linear: $\varphi(\underline{a} + \underline{a}') = \varphi(\underline{a}) + \varphi(\underline{a}')$

$$\varphi(c \cdot \underline{a}) = c\,\varphi(\underline{a})$$

It is surjective since every $g(x) \in \mathbb{F}[x]$ can be written

$$g(x) = \underbrace{f(x)g(x)}_{\in I} + \underbrace{r(x)}_{\deg < n}, \text{ so } r(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$$

for some $a_0, \ldots, a_{n-1} \in \mathbb{F}$

i.e. $\begin{bmatrix} a_0 \\ \vdots \\ a_{n-1} \end{bmatrix} \longmapsto g(x) + I$

It is injective since $\varphi(\underline{a}) = 0 \Rightarrow a_0 + a_1x + \ldots + a_{n-1}x^{n-1} \in I = (f(x))$

$$\Rightarrow a_0 + a_1x + \ldots + a_{n-1}x^{n-1} = \underbrace{f(x)}_{\deg n}\, g(x)$$

$$\Rightarrow a_0 = a_1 = \ldots = a_{n-1} = 0$$

i.e. $\underline{a} = 0$ ▨

REMARK: Same proof shows that if $f(x) \in R[x]$ is monic, then $R^n \longrightarrow R[x]/(f(x))$, $\begin{bmatrix} a_0 \\ \vdots \\ a_{n-1} \end{bmatrix} \longmapsto a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1}$ is a bijection, and abelian group iso.

Just as for groups, this result helps us identify quotient rings...

Noether's 1st Isomorphism Thm (for rings) (Thm 11.4.2): A ring homom. $R \xrightarrow{\varphi} R'$ with $I := \ker\varphi$ induces a ring isomorphism $R/I \xrightarrow{\bar{\varphi}}{}_{\sim} \operatorname{im}\varphi$, $r+I \mapsto \varphi(r)$

proof: Just as easy as for groups (and well-definedness already checked there!):

$\bar{\varphi}$ is a ring homom. since $\bar{\varphi}((a+I)(b+I)) = \bar{\varphi}(ab+I) = \varphi(ab)$
$= \varphi(a)\varphi(b)$
$= \bar{\varphi}(a+I)\bar{\varphi}(b+I)$

actually, we already checked this for groups,
- $\bar{\varphi}$ surjects by defn of imφ!
- $\bar{\varphi}$ injects since $\bar{\varphi}(r+I)=0 \iff \varphi(r)=0$
$\iff r \in \ker\varphi = I$
$\iff r+I = 0+I$ $(=0 \text{ in } R/I)$ ∎

i.e. $R^+ \xrightarrow{\varphi} (R')^+$ induces $R^+/I^+ \to (\operatorname{im}\varphi)^+$ a group isomorphism

EXAMPLES: ("Adjoining roots" = §11.5)

① $2 \in \mathbb{Q}$ has no square root in $\mathbb{Q}$, so I'll try to create a bigger ring (containing $\mathbb{Q}$) where such a root exists:

start with $\mathbb{Q}[x]$, mod out by $I = (x^2-2)$
(i.e. "set $x^2-2=0$ in $\mathbb{Q}[x]$")

giving $\mathbb{Q}[x]/(x^2-2) \cong \mathbb{Q}^2$
($\deg 2$; as $\mathbb{Q}$-vector space, by a previous result)

$a_0 + a_1 x^1 \longleftrightarrow \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$

(Note here, $\alpha := x+I$ has $\alpha^2 - 2 = (x+I)^2 - (2+I) = (x^2-2)+I = I = 0+I = 0$)

In fact, we claim $\mathbb{Q}[x]/(x^2-2) \overset{\sim}{\underset{\text{as rings}}{\cong}} \mathbb{Q}[\sqrt{2}] := \{a+b\sqrt{2} : a,b \in \mathbb{Q}\} \subset \mathbb{R}$ (subfield)

because the homom. $\mathbb{Q}[x] \xrightarrow{\varphi} \mathbb{R}$
sending $x \longmapsto \sqrt{2}$
$f(x) \longmapsto f(\sqrt{2})$

has $\operatorname{im}\varphi = \mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$

$$\left(\text{as } f(x)=a_0+a_1x+a_2x^2+\dots \longmapsto a_0+a_1\sqrt{2}+a_2\cdot 2+a_3\cdot 2\sqrt{2}+a_4 2^2+\dots \right.$$
$$\left. =(a_0+2a_2+4a_4+\dots)+(a_1+2a_3+4a_5+\dots)\sqrt{2}\right)$$

and $\ker\varphi=(x^2-2)$ by our usual argument:

if $f(x)\in\ker\varphi$, write $f(x)=(x^2-2)q(x)+\underbrace{r(x)}_{a+bx}$

$$0=\varphi(f)=f(\sqrt{2})=\underbrace{((\sqrt{2})^2-2)}_{0}q(\sqrt{2})+a+b\sqrt{2}$$

$0=a+b\sqrt{2} \Rightarrow a=b=0$ since $a,b\in\mathbb{Q}$ and $\sqrt{2}\notin\mathbb{Q}$.

i.e. $f(x)\in(x^2-2)$.

Hence by Noether's 1st, $\mathbb{Q}[x]/(x^2-2)\cong\mathbb{Q}[\sqrt{2}]$

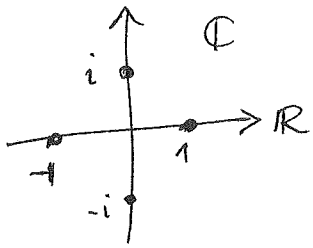
---

(2) Similarly, if we were frustrated that $\mathbb{R}$ has no roots for $x^2+1=0$, i.e. no $\sqrt{-1}$,

we can create the bigger ring $\mathbb{R}[x]/\overbrace{(x^2+1)}^{I}$

where $\alpha := x+I$ does satisfy $\alpha^2=-1$

But then we find $\mathbb{R}[x] \xrightarrow{\varphi} \mathbb{C}$, $x \longmapsto i$



has $\operatorname{im}\varphi=\mathbb{C}$

$\ker\varphi=(x^2+1)\subset\mathbb{R}[x]$

so by Noether's 1st, $\mathbb{R}[x]/(x^2+1)\cong\mathbb{C}$

---

(3) Secretly, this was how we built $\mathbb{F}_4=\{0,1,\alpha,\alpha+1\}$ ($\alpha^3=1$, $\alpha^2=\alpha+1$):

$\mathbb{F}_2=\{0,1\}$ has enough roots to factor the quadratics

$x^2=x\cdot x$ in $\mathbb{F}_2[x]$

$=(x-0)(x-0)$

$x^2+1=(x-1)(x-1)$

$x^2+x=x(x+1)$

$=(x-0)(x-1)$

but not $x^2+x+1=:f(x)$

If we try to create a bigger ring where $x^2+x+1=0$ has a root,

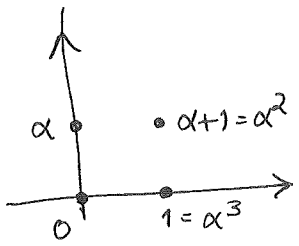
$$\mathbb{F}_2[x]/\underbrace{(x^2+x+1)}_{I} \underset{\text{as } \mathbb{F}_2\text{-vector spaces}}{\simeq} (\mathbb{F}_2)^2$$

$\Downarrow$

$\alpha := x+I$ is a root of x^2+x+1

i.e. $\alpha^2+\alpha+1=0$

or $\alpha^2=\alpha+1$



$\alpha^3 = \alpha\cdot\alpha^2 = \alpha(\alpha+1) = \alpha^2+\alpha = \alpha+1+\alpha = 1$

Can calculate in $\mathbb{F}_4$ multiple ways, e.g.

$\alpha^4 = (\alpha^2)^2 = (\alpha+1)^2 = \alpha^2+2\alpha+1 = \alpha^2+1 = \alpha+1+1 = \alpha$

$\alpha^3\cdot\alpha = \alpha$

$x^2+x+1 \;\big|\; \alpha^4$; $\alpha^4+\alpha^3+\alpha^2$; $\alpha^3+\alpha^2$; $\alpha^3+\alpha^2+\alpha$; α ; quotient $\alpha^2+\alpha$

Interestingly, $\mathbb{F}_2[x]/(x^2+x+1)$ is a field (since $\{1,\alpha,\alpha+1\}$ all have inverses: $\alpha^{-1}=\alpha+1$, $1^{-1}=1$)

and we'll see why this had to be later.

2/8/2019

④ What happens if we try to make $3\in\mathbb{Z}$ invertible by adjoining a root to $3x-1=0$?

i.e. create $\mathbb{Z}[x]/(3x-1)$ as a new ring

↑ not monic, so the structure is trickier!

To understand it, we can try to map

$$\mathbb{Z}[x] \xrightarrow{\varphi} \mathbb{Q}$$

extending $\mathbb{Z}\to\mathbb{Q}$

and $x \longmapsto \frac{1}{3}$

hopefully show $\ker\varphi = (3x-1)$, and identify $\operatorname{im}\varphi \subset \mathbb{Q}$.

Certainly $\ker\varphi \supseteq (3x-1)$

but also if $f(x)\in\ker\varphi$, write $f(x) = (3x-1)\,q(x) = (x-\frac{1}{3})\,\tilde{q}(x)$ with $q(x)\in\mathbb{Q}[x]$

(since $f(\frac{1}{3})=0$)

$f(x) = a_0+a_1x+\dots+a_nx^n$, $a_i\in\mathbb{Z}$

$q(x) = b_0+b_1x+\dots+b_{n-1}x^{n-1}$, $b_i\in\mathbb{Q}$

and then

$$a_0+a_1x+\dots+a_nx^n = \underbrace{-b_0}_{a_0} + \underbrace{(3b_0-b_1)}_{a_1}x + \underbrace{(3b_1-b_2)}_{a_2}x^2 + \dots + (3b_{n-1}-b_n)x^{n-1} + 3b_nx^n$$

$\Rightarrow b_0\in\mathbb{Z}$; $\Rightarrow b_1 = 3b_0-a_1 \in\mathbb{Z}$; $\Rightarrow b_2 = 3b_1-a_2\in\mathbb{Z}$ etc.