(6)

A ring isomorphism $R \xrightarrow{\varphi} R'$ is just a bijective homomorphism.

EXAMPLES: ① $R \xrightarrow{\varphi} \{$ constant polynomials $f(x) \in R[x]\}$ is a ring isomorphism

$a_0 \longmapsto a_0 + 0 \cdot x^1 + 0 \cdot x^2 + \dots$

② $\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} := \{$ integers mod $n\}$

$= \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$

$= \{n\mathbb{Z}, 1+n\mathbb{Z}, 2+n\mathbb{Z}, \dots, n-1+n\mathbb{Z}\}$

$a \longmapsto \bar{a}$

is a surjective ring homomorphism $\left(\begin{array}{l} \overline{a+b} = \bar{a}+\bar{b} \\ \overline{a \cdot b} = \bar{a} \cdot \bar{b} \\ \bar{1} = 1 \text{ in } \mathbb{Z}/n\mathbb{Z} \end{array}\right)$

$\bar{x}$	$\bar{x}^2$
$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$
$\bar{2}$	$\bar{0}$
$\bar{3}$	$\bar{1}$

e.g. $x^2+y^2 = 103$ has no solutions x,y in $\mathbb{Z}$ because it has none in $\mathbb{Z}/4\mathbb{Z}$: $\bar{x}^2, \bar{y}^2 \in \{\bar{0},\bar{1}\}$, so $\bar{x}^2+\bar{y}^2 \in \{\bar{0},\bar{1},\bar{2}\}$

③ Last semester we proved Sun Zi's Theorem, which we could now restate as...

THEOREM: If $\gcd(m,n) = 1$, then

$\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

$\bar{a} \pmod{mn} \longmapsto \left(\bar{a} \pmod{m}, \bar{a} \pmod{n}\right)$

is a ring isomorphism, using the componentwise ring structure on the Cartesian product $R \times R'$ on the right i.e. $(r,r') \cdot (s,s') = (rs, r's')$

$(r,r') + (s,s') = (r+s, r'+s')$

$(0,0) =$ zero

$(1,1) =$ one

1/28/2019>

④ For any choice of some $r_0 \in R$, one gets a substitution homomorphism $R[x] \longrightarrow R$

$f(x) = a_0 + a_1 x + \dots + a_n x^n \longmapsto f(r_0) := a_0 + a_1 r_0 + a_2 r_0^2 + \dots + a_n r_0^n$

Check: $f(x) + g(x) \longmapsto f(r_0) + g(r_0)$

$f(x)g(x) \longmapsto f(r_0)g(r_0)$

$1 \longmapsto 1$

(7)

which is characterized as the unique ring homomorphism

$R[x] \xrightarrow{\varphi} R$

sending constant polynomials $a_0 = a_0 + 0\cdot x + 0\cdot x^2 + \dots \longmapsto a_0$

and sending $x \longmapsto r_0$

Q: Why is it unique?

---

(5) One can combine these ideas, and given $R \xrightarrow{\varphi} R'$ a ring homomorphism, together with a choice of some $r_0' \in R'$, create the unique ring homomorphism

$$R[x] \xrightarrow{\Psi} R'$$

sending $a_0 \longmapsto \varphi(a_0)$ (so extending $R \xrightarrow{\varphi} R'$ on the constants)

$x \longmapsto r_0'$

which forces Ψ to be defined as

$$f(x) = a_0 + a_1 x + \dots + a_n x^n \longmapsto \Psi(f) = \varphi(f)(r_0')$$
$$= \varphi(a_0) + \varphi(a_1) r_0' + \varphi(a_2)(r_0')^2 + \dots + \varphi(a_n)(r_0')^n$$

e.g. $\mathbb{Z}[x] \xrightarrow{\Psi} \mathbb{F}_5 \ (= \mathbb{Z}/5\mathbb{Z})$

extending $\mathbb{Z} \xrightarrow{\varphi} \mathbb{F}_5$ on constants

and substituting $x = \bar{2}$ i.e. $x \xrightarrow{\Psi} \bar{2}$

will send $3x^2 + 6 \xrightarrow{\Psi} \bar{3}\cdot(\bar{2}) + \bar{6} = \overline{6+6} = \overline{12} = \bar{2} \in \mathbb{F}_5$

$f(x) =$

---

(6) One can also create multivariate polynomial rings

$R[x]$

$R[x,y] \ni f(x,y) = a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + a_{02}y^2 + \dots \quad a_{ij} \in R$

$R[x,y,z]$

$R[x_1, x_2, \dots, x_n] \ni f(x_1, \dots, x_n) = \sum_{(i_1, \dots, i_n)} a_{i_1 \dots i_n} x_1^{i_1} \cdots x_n^{i_n}, \quad a_{i_1 \dots i_n} \in R$

with substitution homomorphisms that extend

$$R \xrightarrow{\varphi} R' \quad \text{on constants}$$
$$a_0 \longmapsto \varphi(a_0)$$

and for some choice of $r_1', r_2', \ldots, r_n' \in R'$,

send $x_1 \longmapsto r_1'$
$x_2 \longmapsto r_2'$
$\vdots$
$x_n \longmapsto r_n'$

e.g. $\mathbb{Z}[x,y] \xrightarrow{\Psi} \mathbb{F}_5$

extending $\mathbb{Z} \xrightarrow{\varphi} \mathbb{F}_5$

and substituting $x \longmapsto \bar{0}$
$y \longmapsto \bar{2}$

sends $f(x,y) \xrightarrow{\Psi} \bar{f}(\bar{0},\bar{2})$

e.g. $8 + xy + y^3 \longmapsto \bar{3} + \bar{0}\cdot\bar{2} + (\bar{2})^3 = \overline{3+8} = \bar{11} = \bar{1} \in \mathbb{F}_5$

One has a ring isomorphism, in fact

$$R[x_1,\ldots,x_{n-1},x_n] \xleftarrow{\Psi} \left(R[x_1,\ldots,x_{n-1}]\right)[x_n]$$

extending $R[x_1,\ldots,x_{n-1},x_n] \xleftarrow{\varphi} R[x_1,\ldots,x_{n-1}]$

$f(x_1,\ldots,x_{n-1}) \longleftarrow f(x_1,\ldots,x_{n-1})$

and substituting $x_n \longleftarrow 1 \; x_n$

whose inverse map is simply "grouping by powers of x_n"

e.g. $\mathbb{Z}[x,y] \xleftarrow{\Psi} (\mathbb{Z}[x])[y]$

$8 + xy + y^3 + x^4y \longleftarrow 8 + (x+x^4)y^1 + 0\cdot y^2 + 1\cdot y^3$

⑦ (PROP 11.3.10) every ring R has a unique (!) (ring) homomorphism $\mathbb{Z} \xrightarrow{\varphi} R$

because it must send $1 \longmapsto 1 = \varphi(1)$

and hence $n = \underbrace{1+1+\cdots+1}_{n \text{ times}} \longmapsto \varphi(n) = \varphi(1)+\cdots+\varphi(1) = 1+\cdots+1$

and $-n \longmapsto -\varphi(n) = -(1+\cdots+1)$

Since $\mathbb{Z}^+ \xrightarrow{\varphi} R^+$ is an (abelian) group homomorphism,

$\ker(\varphi) = \varphi^{-1}(0)$ is a subgroup of $\mathbb{Z}^+$, so one of $\{n\mathbb{Z}\}_{n>0}$, $\{0\}$

hence either ...

DEF'N: $\ker(\mathbb{Z} \xrightarrow{\varphi} R) = \begin{cases} n\mathbb{Z} \text{ and we say } R \text{ has characteristic } n \\ \quad \text{i.e. } n = \text{smallest positive integer for which } 1+1+\cdots+1=0 \\ \text{or} \\ \{0\} \text{ and we say } R \text{ has characteristic } 0 \end{cases}$

---

	ring	characteristic
e.g.	$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$	0
	$\mathbb{Z}/n\mathbb{Z}$	n
	$R \subset R[x] \subset R[x,y] \subset \cdots$	same as characteristic of R

Thinking about this a bit will already help us see why finite fields $\mathbb{F}$ have $|\mathbb{F}| = p^n$...

DEF'N: Say a ring R is a domain (or integral domain) if $ab=0$ in R implies $a=0$ or $b=0$

equivalently, $a,b \in R-\{0\} \Rightarrow ab \in R-\{0\}$

EXAMPLES: ① Fields $\mathbb{F}$ are domains, since if $ab=0$ and $a \neq 0$

then $\bar{a}^{-1} \cdot ab = \bar{a}^{-1} \cdot 0$

$b = 0$

NONEXAMPLE: $\mathbb{Z}/mn\mathbb{Z}$ has $\bar{m} \neq 0$, $\bar{n} \neq 0$, but $\bar{m} \cdot \bar{n} = 0$

② Subrings of fields are always domains for same reason

$R \subset \mathbb{F}$

e.g. $\mathbb{Z} \subset \mathbb{Q}$

$\mathbb{Z}[i] \subset \mathbb{C}$

(and later (§11.7) we'll see every domain R is a subring of a field, its field of fractions)

③ R a domain $\Rightarrow R[x]$ a domain, since $f(x) = a_0 + \cdots + a_n x^n$ with $a_n \neq 0$, $g(x) = b_0 + \cdots + b_m x^m$ with $b_m \neq 0$

has $(fg)(x) = a_0 b_0 + \cdots + a_n b_m x^{n+m}$ with $a_n b_m \neq 0$.

PROPOSITION: A domain R (and hence every field) has characteristic either a prime p or characteristic 0
(like $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$) ((like $\mathbb{Q}, \mathbb{R}, \mathbb{C}$)

proof: Given a domain R, if characteristic is $n \neq 0$ and n is not prime, say $n = n_1 n_2$

then $0 = \underbrace{1+1+\dots+1}_{n \text{ times}} = \underbrace{(1+\dots+1)}_{n_1 \text{ times}} \underbrace{(1+\dots+1)}_{n_2 \text{ times}}$ ← use distributivity

forces either $\overbrace{1+\dots+1}^{n_1} = 0$, i.e. R has smaller characteristic! ∎

or $\underbrace{1+\dots+1}_{n_2}$

1/30/2019

COROLLARY: Every finite field $\mathbb{F}$ has characteristic a prime p, and $|\mathbb{F}| = p^d$ for some $d \geq 1$.

proof: In $\mathbb{F}$, the sequence $1, \frac{1+1}{2}, \frac{1+1+1}{3}, \dots$ must eventually repeat since $|\mathbb{F}| < \infty$, and if $m = n$ for some $m < n$ then $-m+m = -m+n$, so $\mathbb{F}$ has characteristic not 0, $\overset{\|}{0}$ which must be a prime p by PROP above.

We claim then that every $\alpha \in \mathbb{F}$ has $p\alpha := \underbrace{\alpha+\alpha+\dots+\alpha}_{p \text{ times}} = 0$

since $p\alpha = (1+1+\dots+1)\alpha$
$= 0 \cdot \alpha = 0$

and therefore we can make $\mathbb{F}^+ = (\mathbb{F}, +)$ into a vector space over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{(p-1)}\}$

by defining the scaling $\mathbb{F}_p \times \mathbb{F} \longrightarrow \mathbb{F}$

$(\bar{m}, \alpha) \longmapsto \bar{m} \cdot \alpha = \underbrace{\alpha+\dots+\alpha}_{m \text{ times}}$

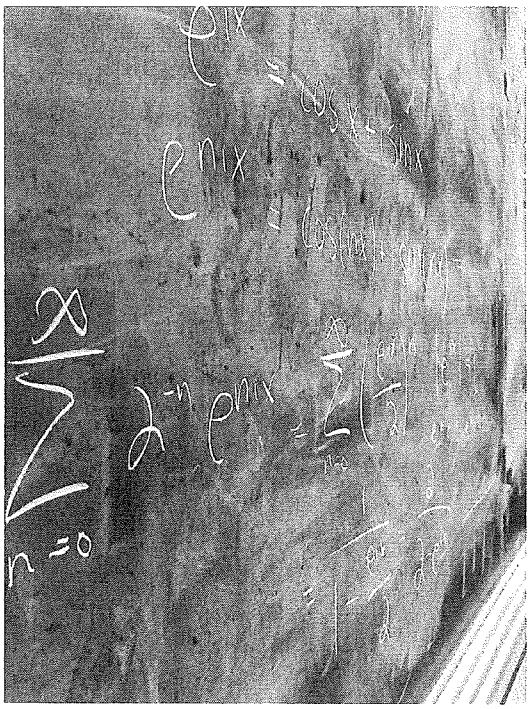
(Checking well-defined-ness is the trickiest part; rest is easy)

$\bar{m}_1 = \bar{m}_2 \Rightarrow \bar{m}_1 \cdot \alpha = \bar{m}_2 \cdot \alpha$

Undergraduate Mathematics Research Seminar

University of Minnesota
School of Mathematics

- ➢ Come hear about the research that undergraduates do in the mathematics department
- ➢ Present on the mathematics research you do
- ➢ Present on a paper you think would be interesting
- ➢ Present on a cool topic you learned about in class



When: **Tuesdays, 12:30PM**
Where: **301 Vincent Hall**
Who: **Any undergraduate student is welcome!**

For details, email chand409@umn.edu.