1/25/2019
(4)

EXAMPLES

$\mathbb{Z}[i] := \{a+bi : a,b\in\mathbb{Z}\}$ (ring, subring of $\mathbb{Q}[i]$, subfield of $\mathbb{C}$) $\subset \mathbb{Q}[i] := \{a+bi : a,b\in\mathbb{Q}\}$ (field, subfield of $\mathbb{C}$) $\subset \mathbb{C} = \{a+bi : a,b\in\mathbb{R}\}$

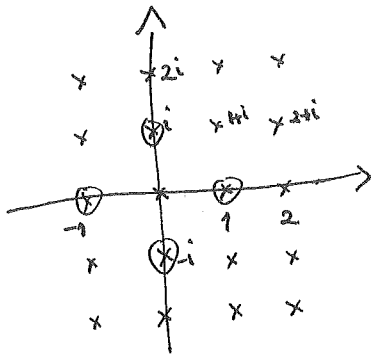
(1)

$\mathbb{Z}$ (ring) $\subset$ $\mathbb{Q}$ (field) $\subset$ $\mathbb{R}$ (subfield, field) $\subset$ $\mathbb{C}$ (subfield, field) $\subset$ $\mathbb{H}$ (subring, noncomm. ring)

$\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} : a,b\in\mathbb{Z}\}$ (subring of $\mathbb{Q}[\sqrt{2}]$) $\subset \mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} : a,b\in\mathbb{Q}\}$ (a field by EXERCISE 3.2.1)

$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2}$

$\mathbb{Z}[i] := \{a+bi : a,b\in\mathbb{Z}\}$ are called the Gaussian integers



On midterm exam 2 in fall, we showed $\mathbb{Z}[i]^\times = \{+1,-1,+i,-i\}$

$\mathbb{Z}[\sqrt{2}]^\times$ behaves differently, in that it is infinite,

e.g. $-(1+\sqrt{2})(1-\sqrt{2}) = -(1-2) = 1$, so $\pm(1\pm\sqrt{2})^n \in \mathbb{Z}[\sqrt{2}]^\times \ \forall n$

(2) Given any ring R, we can create a new one...

DEF'N: $R[x] :=$ polynomials in x with coefficients in R

$$:= \left\{ f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n : a_0,\dots,a_n \in R \right\}$$

" $\sum_{i=0}^{n} a_i x^i$

with addition, mult. defined as follows: $+$ $\times$

if $g(x) = b_0 + b_1x + \dots + b_mx^m = \sum_{j=0}^{m} b_jx^j$

then $f(x)+g(x) = (a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+\dots+(a_N+b_N)x^N$ where $N=\max(n,m)$

$$= \sum_{i=0}^{\max(n,m)} (a_i+b_i)x^i$$

(5)

$$f(x)g(x) = a_0b_0 + (a_0b_1+a_1b_0)x^1 + (a_0b_2+a_1b_1+a_2b_0)x^2 + (a_0b_3+a_1b_2+a_2b_1+a_3b_0)x^3 + \dots + (a_{m-1}b_{n-1}+a_mb_{n-1}+a_{m-1}b_n)x^{m+n-1} + a_nb_mx^{m+n}$$

$$= \sum_{k=0}^{m+n} c_k x^k \quad \text{where } c_k = \sum_{\substack{(i,j):\\ i+j=k}} a_ib_j$$

---

e.g. In $\mathbb{Z}[x]$, $f(x) = 4+3x^2$ have $f+g = 9+7x+3x^2+x^4$

$g(x) = 5+7x+x^4$ $\quad f\cdot g = (4+3x^2)(5+7x+x^4)$

$= 20+28x+21x^3+4x^4+3x^6$
$\quad +15x^2$

It's a bit tedious to check carefully that this $+, \times$ make $R[x]$ a ring (mostly associativity of $\times$ is a bit of a pain), but lets at least note who $0, 1$ are, namely they're special cases of the constant polynomials $\{f(x) = a_0\}$ for $a_0 \in R$
$= a_0 + 0\cdot x + 0\cdot x^2 + 0x^3 + \dots$

which is a subring of $R[x]$, isomorphic to R

So $0 = 0 + 0\cdot x + 0\cdot x^2 + \dots \in R[x]$
$1 = 1 + 0\cdot x + 0\cdot x^2 + \dots \in R[x]$

What did this word mean?

DEF'N: (11.3.1) Given rings R, R', a map $R \xrightarrow{\varphi} R'$ is a homomorphism if it respects $+, \times, 1$, i.e.,

- $\varphi(a+b) = \varphi(a)+\varphi(b)$ (EXERCISE: This forces $\varphi(0)=0$ and φ is an abelian group homomorphism $R^+ \to (R')^+$)
- $\varphi(ab) = \varphi(a)\varphi(b)$
- $\varphi(1) = 1$

needs to be required separately, e.g. the zero map $R \xrightarrow{\varphi} R'$, $r \mapsto 0$ $\forall r \in R$ satisfies 1st two conditions but not third, unless $R' = \{0\}$.

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

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

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 $R[x] \longrightarrow R$

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

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

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

$1 \longmapsto 1$