

(§ 16.2) Integral Domains & Fields

Recall: If R is a ring, and $r \neq 0$ is in R , then we call r a zero divisor if $\exists s \in R, s \neq 0$ s.t. $rs = 0$.

An integral domain is a commutative ring w/ identity that has no zero divisors.

A field is a commutative division ring.



a particular kind
of integral domain

$\forall a \in R, a \neq 0$ has
 $a^{-1} \in R$ s.t. $aa^{-1} = a^{-1}a = 1$

unity

Examples:

($\forall a, b \in F$ s.t. $ab = 0$,
if we let $a \neq 0 \Rightarrow a^{-1}ab = a^{-1}0$
 $\Rightarrow b = 0$)

the only units
of \mathbb{Z} are ± 1

① \mathbb{Z} is an integral domain (but not a field).

② Ring w/ unity \mathbb{Z}_7 has no zero divisors.

If $ab \equiv 0 \pmod{7}$, then $7 \nmid ab$ (7 -prime) \Rightarrow

$7 \mid a$ or/and $7 \mid b$ in $\mathbb{Z}_7 \Rightarrow a \equiv 0 \pmod{7}$ or $b \equiv 0 \pmod{7}$

So, \mathbb{Z}_7 is an integral domain (and a field!) \hookrightarrow why?

Recall: \mathbb{Z}_{12} is not an integral domain:

$3 \cdot 4 \equiv 0 \pmod{12}$, $3 \neq 0, 4 \neq 0$ ($\Rightarrow \mathbb{Z}_{12}$ is not a field)

zero divisors!

③ $\mathbb{Z}[x]$, the ^{commutative} ring of polynomials w/ integer coefficients, is an integral domain:

Set $f, g \in \mathbb{Z}[x]$ w/ $fg = 0$ then $f = 0$ or $g = 0$.

Proof: if both $f \neq 0$ and $g \neq 0 \Rightarrow$
 $\deg(fg) = \deg f + \deg g \geq 0 \Rightarrow fg \neq 0 \Rightarrow$ a contradiction

($\deg(0)$ is undefined)

$\mathbb{Z}[x]$ is not a field: for example, if $g(x) = x$
has $\bar{g}(x) \in \mathbb{Z}[x]$ s.t. $x\bar{g}(x) = 1 \Rightarrow$ we have a contradiction $0 = 1$
at $x = 0$.)

④ $\mathbb{Z}[i] = \{a+bi, a, b \in \mathbb{Z}\}$ is a ring known as the Gaussian integers.

②

$\mathbb{Z}[i]$ is a subring of \mathbb{C} and an integral domain. (D/R)
(field)

Why? Suppose $x, y \in \mathbb{Z}[i]$ s.t. $xy = 0$. Let

$$x = a+bi, y = c+di \Rightarrow 0 = xy = (a+bi)(c+di)$$

$$= (ac-bd) + (ad+bc)i \Rightarrow ac-bd=0 \\ ad+bc=0$$

If $c=0$ $\Rightarrow bd=0$ and $ad=0$. If $d=0$ \Rightarrow

$c+di = 0+0i = 0$ $\Rightarrow y=0$ we are done.

If $d \neq 0 \Rightarrow b=0$ and $a=0 \Rightarrow a+bi=0+0i=0$

$\Rightarrow x=0$ we are done.

If $c \neq 0$ $\Rightarrow a = \frac{bd}{c} \Rightarrow ad = \frac{bd^2}{c} = -bc \Rightarrow$
 $bd^2 = -bc^2$. If $b \neq 0 \Rightarrow d^2 = -c^2$, but both

$d^2, c^2 \geq 0 \Rightarrow d^2 = -c^2$ only when $d=c=0$; but

since $c \neq 0$, hence $b=0$. Then $a = \frac{bd}{c} = \frac{0}{c} = 0 \Rightarrow x=0$

Ex. 6.12

In all cases, either $x=0$ or $y=0$ and hence

$\mathbb{Z}[i]$ is an integral domain. \square

$\mathbb{Z}[i]$ is not a field:
 $\nexists x \in \mathbb{Z}[i]$ s.t.
 $x \neq 0$ $x(1+0i) = 1+0i = 1$

⑤ $\mathbb{Z} \times \mathbb{Z} = \{(m, n) \mid m, n \in \mathbb{Z}\}$

$$(m, n) + (p, q) = (m+p, n+q) \\ (m, n)(p, q) = (mp, nq)$$

additive id = $(0, 0)$
mult. id = $(1, 1)$

commutative ring w/ unity
note: it is not an integral domain:

$$(x, 0) \cdot (0, y) = (0, 0) \text{ with } x \neq 0, y \neq 0.$$

see in text
 $\mathbb{Z}[i]$ is not a field!
(only units are $\pm 1, \pm i$)
why?

⑥ The set of matrices

$F = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$ (w/ entries in \mathbb{Z}_2)
 forms a field.

F closed under addition/multiplication,

F is a commutative ring w/ unity $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$$\text{e.g., } \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \text{ etc.}$$

and $\exists A^{-1}$ for each $A \in F$, e.g., see example above.
 $(A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix})$

⑦ Consider the set $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

It is a field (commutative division ring)

w/ unity $1+0\sqrt{2}=1$ with $+$ & \times of real #'s:

- $\mathbb{Q}[\sqrt{2}]$ is closed under addition

$$(a+b\sqrt{2}) + (c+d\sqrt{2}) = (a+c) + (b+d)\sqrt{2}$$

and multiplication:

$$\begin{aligned} (a+b\sqrt{2})(c+d\sqrt{2}) &= ac + ad\sqrt{2} + bc\sqrt{2} + bd(\sqrt{2})^2 \\ &= (ac+bd) + (ad+bc)\sqrt{2} \end{aligned}$$

- Addition is associative and commutative in $\mathbb{Q}[\sqrt{2}]$.

- Additive identity: $0+0\sqrt{2}=0 \in \mathbb{Q}[\sqrt{2}]$.

- Additive inverses: $\forall a+b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$,

$\exists -(a+b\sqrt{2}) \in \mathbb{Q}[\sqrt{2}]$ s.t. $(a+b\sqrt{2}) - (a+b\sqrt{2}) = 0$

- Multiplication is associative & commutative in $\mathbb{Q}(\sqrt{2})$.

- Distributivity holds.

- Multiplicative identity: $1=1+0\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$

- Multiplicative inverses: need to show that
 for $a+b\sqrt{2} \neq 0$ ($a, b \in \mathbb{Q}$) and either $a \neq 0$ or $b \neq 0$

$\exists c, d \in \mathbb{Q}$ s.t. $(a+b\sqrt{2})(c+d\sqrt{2})=1$. (7)

Consider $\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2-2b^2}$

$$= \underbrace{\frac{a}{a^2-2b^2}}_{\in \mathbb{Q}} - \underbrace{\frac{b}{a^2-2b^2}}_{\in \mathbb{Q}} \cdot \sqrt{2} \in \mathbb{Q}[\sqrt{2}], \text{ so}$$

$$c = \frac{a}{a^2-2b^2}, \quad d = -\frac{b}{a^2-2b^2}.$$

Q: Why $a^2-2b^2 \neq 0$?

Thus, $\mathbb{Q}[\sqrt{2}]$ is a field. □

Proposition (16.15)

Cancellation Law:

used for
defining
integral domains
in some texts

Let R be a commutative ring w/ identity.
Then R is an integral domain if and only if
for all $a \in R$, $a \neq 0$ w/ $ab = ac \Rightarrow b = c$.

Proof: \Rightarrow Let R be an integral domain, Then
(no zero divisors)

$\forall a \in R$, $a \neq 0$, $ad = 0 \Rightarrow d = 0$. Let $ab = ac \Rightarrow$

$$ab - ac = 0 \Rightarrow a(b - c) = 0 \underset{a \neq 0}{\Rightarrow} b - c = 0 \Rightarrow b = c.$$

\Leftarrow Let $a \neq 0$, $ab = ac \Rightarrow b = c$.

Then if $ad = 0 = ac$ (a $\neq 0$) $\Rightarrow d = c \Rightarrow R$ has no

zero divisors $\Rightarrow R$ is an integral domain. □

Theorem (16.16) Every finite integral domain
is a field.

comm. ring w/ id, no zero
divisors

Proof: Let D be a finite integral domain and
let identity in D be 1 .
Show that $\forall a \neq 0$, $a \in D$, a is a unit.

also proof
in textbook

Case 1: $a = 1 \Rightarrow a^{-1} = a = 1$

Case 2: $a \neq 1 \Rightarrow$ consider the sequence a, a^2, a^3, \dots finite

(5)

Since D is finite, then \exists integers $i, j \geq 0$ s.t. $i > j$ and $a^i = a^j$. Then $a^i = a^{i-j+j} = a^{i-j}a^j = a^j$, that is, $a^{i-j}a^j = 1 \cdot a^j \stackrel{\text{(by cancellation)}}{=} a^{i-j} = 1 \Rightarrow$ (recall $a \neq 1$ and $i-j > 0$) $a^{i-j-1}a = a^{i-j} = 1 \Rightarrow a^{-1} = a^{i-j-1}$. That is, $\forall a \neq 0 \exists a^{-1} \Rightarrow D$ is a field \square

As a corollary : for every prime p , \mathbb{Z}_p is a field

$\left\{ \begin{array}{l} \text{(ring) } \mathbb{Z}_p \text{ is finite \& } \mathbb{Z}_p \text{ is an integral domain} \\ (\text{if } a, b \in \mathbb{Z}_p \text{ s.t. } ab \equiv 0 \pmod{p} \Rightarrow \text{for some integer } k, ab = pk, \text{i.e. } p \mid ab \Rightarrow p \mid a \text{ or } p \mid b \Rightarrow a=0 \text{ or } b=0) \\ (\text{p prime}) \end{array} \right.$

\Rightarrow by Thm. 16.16, \mathbb{Z}_p is a field. \square

Def: The characteristic of a ring R is the least pos. integer n s.t. $nr (= \underbrace{r+r+\dots+r}_n) = 0 \quad \forall r \in R$ and we write $\boxed{\text{char } R = n}$.

If \nexists such $n \Rightarrow \boxed{\text{char } R = 0}$

Examples: (1) \forall prime p , \mathbb{Z}_p is a field w/ $\text{char } \mathbb{Z}_p = p$,
 $(\forall a \neq 0, a \in \mathbb{Z}_p, pa = \overbrace{a+a+\dots+a}^p = 0 \pmod{p})$

(2) $\text{char } \mathbb{Z} = 0$; (3) $\text{char } \mathbb{Z}_n = n$ (see Example (1))

Lemma (16.18) : Let R be a ring w/ unity 1 . Then if 1 has infinite order under addition $\Rightarrow \text{char } R = 0$. If 1 has order n under addition $\Rightarrow \text{char } R = n$.

(6)

Proof: If $|1| = \infty \Rightarrow \nexists n > 0$, integer s.t.

$n \cdot 1 = 0 \Rightarrow \text{char } R = 0$ by def. of $\text{char } R$.

If $|1| = n \Rightarrow n \cdot 1 = 0 \Rightarrow n \frac{r}{n} \in R = n(1 \cdot r) = (n \cdot 1)r = 0 \cdot r = 0 \Rightarrow \nexists r \in R, \exists n > 0$ integer s.t.

$n r = 0 \Rightarrow \text{char } R = n$. \square

Theorem (16.19) The characteristic of an integral domain is either prime or zero.

Proof: Let D be an integral domain.

Then $\text{char } D = 0$ or $\text{char } D \neq 0$. If $\text{char } D \neq 0$ and, say, $\text{char } D = n$, where n is not prime \Rightarrow

$n = ab$, $1 < a < n$, $1 < b < n$. Consider $n \cdot 1 = 0$

$$\Rightarrow 0 = n \cdot 1 = (ab)1 = (a \cdot 1)(b \cdot 1) \Rightarrow a \cdot 1 = 0 \text{ or } b \cdot 1 = 0$$

(D is an integral domain)

$\Rightarrow \text{char } D < n \Rightarrow$ a contradiction. So, n is prime,

and, therefore, $\text{char } D = \text{prime} \#$. \square

Examples:

$\rightarrow \oplus$ & \otimes are done as for polynomials in $\mathbb{Z}[x]$, but mod 2

1) $\mathbb{Z}_2[x]$ comm. ring of polynomials w/ coeff's in \mathbb{Z}_2 w/ unity $p(x) \equiv 1$.

($\text{char } \mathbb{Z}[x] = 0$) $|1| = \infty$ $\text{char } \mathbb{Z}_2[x] = 2$. Why? Note: $|1| = 2$

since $2 \cdot 1 = 2 \equiv 0 \pmod{2} \Rightarrow$ use lemma 16.18

2) $\text{char } R = \text{char } \mathbb{K} = \text{char } \mathbb{Q} = \text{char } \mathbb{C} = 0$

(field) (int. domain) (field) (field) " $(n \cdot 1 = 1 + 1 + \dots + 1 = 0 \text{ iff } n = 0, |1| = \infty)$ $\text{char } \mathbb{Q}[\mathbb{F}_2]$