Abstract Algebra Notes Day 10 & 11 Notes Fall 2025

(Ch 12 Gallian) Intro to Rings

Def A nonempty set R together with two binary operations,

additions and multiplication,

is a ring if the following holds.

1. $(R, +)$ is an abelian group w/ identity called zero 0

   This means :

   - $a+b=b+a$ for $a,b \in R$
   - $(a+b)+c = a+(b+c)$ for all $a,b,c \in R$
   - there is $0 \in R$ with $a+0=a$ for all $a \in R$
   - For every $a \in R$, there is $-a \in R$ with $a+(-a)=0$

2. Multiplication is associative

   This means:

   $(ab)c = a(bc)$ for $a,b,c \in R$

3. The following distributive property holds:

   For $a,b,c \in R$,

$$a(b+c) = ab+ac$$
$$(a+b)c = ac+bc$$

Def

- R is a ring with unity or with identity if there is an elt $1 \in R$ such that $1 \neq 0$ and $1a = a1 = a$ for each $a \in R$

- R is a commutative ring if $ab = ba$ for all $a, b \in R$
(if multiplication is commutative)

Def An elt $a \in R$ is a zero divisor if

- a is not the zero elt
- there is a nonzero elt $b \in R$ such that $ab = 0$

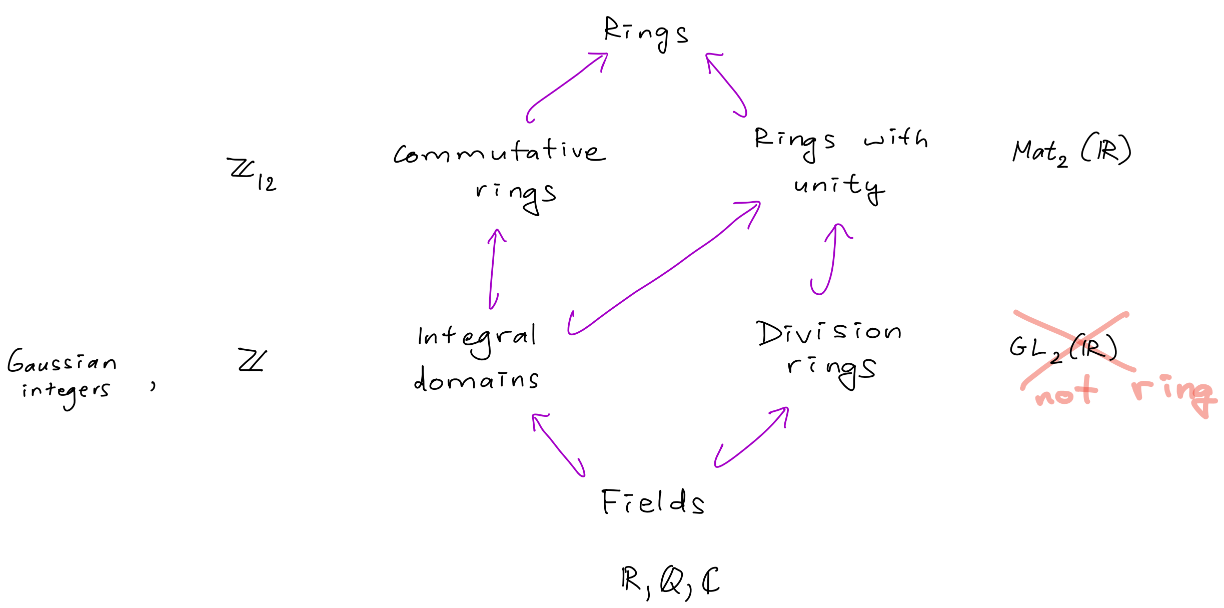
Def A nonzero elt $a \in R$ where R is a ring with unity is a unit if there exists a unique elt $a^{-1} \in R$ such that $a^{-1}a = aa^{-1} = 1$.

Def

- A commutative ring with unity R is called an integral domain if R has no zero divisor.

- A ring with unity R is a division ring if every nonzero elt in R is a unit

- A division ring which is commutative is a field



Ex $\mathbb{Z}$ is an integral domain

(if $ab=0$ for two integers a and b, either $a=0$ or $b=0$)

$\mathbb{Z}$ is not a division ring

(the only integers with multiplicative inverses are 1 and -1),

so $\mathbb{Z}$ is not a field

Ex of fields:

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ under the ordinary addition and multiplication

Ex $\mathbb{Z}_n$ with the usual addition and multiplication mod n is a commutative ring with unity 1.

The set of units is $U(n) = \{\text{nonzero } a \in \mathbb{Z}_n : \gcd(a,n)=1\}$

Ex In $\mathbb{Z}_{12}$, we have $3 \cdot 4 = 0$.

So 3 and 4 are zero divisors.

$\mathbb{Z}_{12}$ is a Commutative ring which is not an integral domain

Ex The set S of continuous functions $f : [a,b] \to \mathbb{R}$

with addition

$(f+g)(x) = f(x) + g(x)$ (called "point-wise addition")

and multiplication

$(fg)(x) = f(x)\, g(x)$ (called "point-wise multiplication")

forms a commutative ring with unity.

The unity is the constant function 1

The zero elt is the constant function 0.

Ex $\mathrm{Mat}_2(\mathbb{R}) = \{ 2 \times 2$ matrices with entries in $\mathbb{R} \}$

forms a non-commutative ring with unity under the usual matrix addition and matrix multiplication.

The unity is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

The zero elt is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

$\mathrm{Mat}_2(\mathbb{R})$ has zero divisors, e.g. $\begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

Prop of rings   Let R be a ring with $a, b \in R$.

(Prop 16.8)   ① $\underset{\uparrow}{a\,0} = 0$ and $\underset{\nearrow}{0\,a} = 0$ (0 is the zero elt of the ring)

ring multiplication

② $a(-b) = -(ab)$ and $(-a)b = -(ab)$

③ $(-a)(-b) = ab$

Proof ① $a0 = a(0+0)$ since 0 is the identity elt of $(R,+)$

$= a0 + a0$ by the distributivity property

So $a0$ is the identity elt of $(R,+)$,

and thus $a0 = 0$.

Exercise: Show $0a = 0$

② $ab + a(-b) = a(b-b)$ by the distributive property

$= a0$

$= 0$ by part (1)

So the additive inverse of ab is $a(-b)$

meaning $-(ab) = a(-b)$

Exercise: Show $(-a)b = -(ab)$.

③ Exercise : Show $(-a)(-b) = ab$.

Subring check Let R be a ring and $S \overset{\text{Subset}}{\subseteq} R$. Then

S is a subring of R iff all conditions hold:

Showing $(S,+)$ is a subgroup of $(R,+)$

- $0 \in S$
- $x+y \in S$ for all $x,y \in S$ (S is closed under ring addition)
- $-x \in S$ for all $x \in S$ (S is closed under negation)
- $xy \in S$ for all $x,y \in S$ (S is closed under ring multiplication)

Ex $2\mathbb{Z} = \{2k : k \in \mathbb{Z}\}$ is a subring of $\mathbb{Z}$.

Note: $2\mathbb{Z}$ is a commutative ring without unity

although $\mathbb{Z}$ ——— " ——— with unity 1

Ex Let T be the set of upper-triangular matrices in $Mat_2(\mathbb{R})$

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a,b,c \in \mathbb{R} \right\}.$$

Then T is a subring of $Mat_2(\mathbb{R})$.

T is closed under matrix multiplication:

Given $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, $B = \begin{pmatrix} d & e \\ 0 & f \end{pmatrix}$, $AB = \begin{pmatrix} ad & ae+bf \\ 0 & fc \end{pmatrix} \in T$.

Group exercise: Why is $GL_2(\mathbb{R})$ not a subring of $Mat_2(\mathbb{R})$?

Ex Both $\{0\}$ and R are subrings of any ring R.

$\{0\}$ is called the trivial subring of R

Ex $\{0,2,4\}$ is a subring of the ring $\mathbb{Z}_6$.

Note: Although 1 is the unity of $\mathbb{Z}_6$,

4 is the unity in $\{0,2,4\}$: $(2)(4)=2$ and $(4)(4)=4$ and $(0)(4)=0$.

(Ch 13 Gallian) Integral domains (and fields)

Ex · The set of <u>Gaussian integers</u>

$$\mathbb{Z}[i] \overset{def}{=} \{a+bi : a,b \in \mathbb{Z}\}$$

is a subring of $\mathbb{C}$ (Verify the subring conditions)

- Check $\mathbb{Z}[i]$ is an integral domain

- The only units in $\mathbb{Z}[i]$ are $1, -1, i, -i$. <u>Ex</u> $(i)(-i) = -i^2 = -(-1) = 1$

<u>Why?</u>

Suppose $x = a+bi \in \mathbb{Z}[i]$ is a unit with inverse $y = c+di$

$$1 = xy = (a+bi)(c+di) = ac + adi + bci - bd$$

so $ad - bd = 1$ and $ad + bc = 0$

Then its conjugate $\bar{x} = a - bi$ is also a unit with inverse $\bar{y} = c - di$

because $\bar{x}\bar{y} = (a-bi)(c-di) = ac - adi - bci - bd = 1 - 0i = 1$

Thus $1 = 1 \cdot 1 = (xy)(\bar{x}\bar{y}) = x\bar{x} \; y\bar{y} = (a^2+b^2)(c^2+d^2)$

Since $a,b,c,d \in \mathbb{Z}$, we know a^2+b^2 must be either 1 or -1.

So $a+bi$ is either $1, -1, i$, or $-i$.

The other nonzero elts of $\mathbb{Z}[i]$ are not units,
e.g. $1+2i$ is not a unit.

So $\mathbb{Z}[i]$ is not a field

Ex The set of matrices

$$F = \left\{ \overbrace{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}^{\text{the unity}}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \overbrace{\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}}^{\text{the zero elt}} \right\} \subset Mat_2(\mathbb{Z}_2)$$

with entries in $\mathbb{Z}_2$ forms a field

under usual matrix addition and multiplication.

For example: $\underset{x}{\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}} \underset{y}{\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

So both x and y are units in F

—— end of Day 10 notes ——

(Start of Day 11 notes:)

Prop (Cancellation law for integral domain)

Let D be an integral domain, with $a, b, c \in D$.

If a is nonzero and $ab = ac$,

then $b = c$

Proof From $ab = ac$, we have

$0 = ab - ac$

$= a(b-c)$ by the distributivity property

Since D has no zero divisors (by def of integral domain),

$a = 0$ or $b - c = 0$.

Since $a \neq 0$ by assumption,

$b - c = 0$

$b = c$, $\square$

Thm Every finite integral domain is a field

Proof Let D be a finite integral domain

(D is a commutative ring with unity 1, and D has no zero divisors)

Let a be a nonzero elt in D

(We need to show that a is a unit, meaning $ab=1$ for some elt $b \in D$)

If $a=1$, then a is its own (multiplicative) inverse.

Suppose $a \neq 1$. Consider the sequence of elts in D

$$a, \ a^2, \ a^3, \ \ldots$$

Since D is finite, there must be two positive integers i, j with $i<j$ such that $a^i = a^j$.

$$a^i 1 = a^i a^{j-i}$$

By the above prop (Cancellation fos integral domain),

$$1 = a^{j-i}$$

Since $a \neq 1$, we know $j-i > 1$.

This means $1 = a\, a^{j-i-1}$

so a^{j-i-1} is the inverse of a $\square$

Notation For any non negative integer n and elt $x \in R$, write $\underbrace{x + x + \cdots + x}_{n \text{ times}}$ as nx or $n \cdot x$

Warning This could potentially be confusing because we write

sr

to denote the product $\overset{\text{ring multiplication operation}}{sr}$ for $s, r \in R$

Def The <u>order</u> of an elt x in a ring R is the order of x under the addition operation of R, i.e. the order of x as group elt $(R, +)$,

Recall

i.e. the smallest positive integer n such that

$$n \cdot x = 0$$

If no such integer exists, say x has infinite order

Def The <u>characteristic</u> of a ring R,

$$\text{char } R,$$

is the smallest positive integer n such that $n.x = 0$ for $\underline{\underline{\text{all}}}$ $x \in R$.

If no such integer exists, then we define $\text{char } R = 0$.

Ex The rings $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}, \mathbb{Z}[i]$

all have characteristic 0 because

there is no positive integer n such that $n \cdot 1 = 0$

Ex The ring $\text{Mat}_2(\mathbb{R})$ also has char 0.

The order of unity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is infinite.

Ex For every prime p, $\mathbb{Z}_p$ is a field of char p.

Proof that $\mathbb{Z}_p$ is a field

$\gcd(x, n) = 1$ iff

x has a multiplicative inverse in mod n

So every elt of $\mathbb{Z}_p$ (except 0) is a unit.

Proof that $\mathbb{Z}_p$ has characteristic p:

The order of the unity elt 1 is p

$\square$

Lemma Let R be a ring with unity 1.

(a) If 1 has order n, then char $R = n$

(b) If 1 has infinite order, then char $R = 0$.

group
activity
Day 11
&
also
next
HW

Proof Suppose 1 has order n,

then n is the smallest positive integer such that $n \cdot 1 = 0$.

Then, for all $r \in R$,

$$n \cdot r = n \cdot (1r) \quad \text{by def of unity}$$

$$= \underbrace{1r + 1r + \dots + 1r}_{n \text{ times}} \quad \text{(what the notation means)}$$

$$= \underbrace{(1 + \dots + 1)}_{n \text{ times}} r \quad \text{by the distributive property}$$

$$= 0\, r \quad \text{since } n \cdot 1 = 0$$

$$= 0 \quad \text{by def of the zero elt}$$

If 1 has infinite order, then no positive n exists such that $n \cdot 1 = 0$. By def, char R is 0. □

(Extra notes)

$\boxed{\text{Lemma } \star}$ $(m \cdot x)(n \cdot y) = (mn) \cdot (xy)$ for $m, n \in \mathbb{Z}$, $x, y \in R$

Proof (Partial proof, for positive m and n)

$$(m \cdot x)\underset{\substack{\uparrow \\ \text{ring} \\ \text{multiplication}}}{}(n \cdot y) = (\underbrace{x + x \cdots + x}_{m \text{ times}})(\underbrace{y + y + \cdots + y}_{n \text{ times}})$$

$$= \underbrace{xy + xy + \quad \cdots \quad + xy}_{mn \text{ times}} \qquad \text{(by foiling)}$$

$$= (mn) \cdot (xy)$$

Thm The characteristic of an integral domain is either prime or zero.

Proof Let D be an integral domain.

Suppose char $D = c$ with $c \neq 0$.

For the sake of contradiction, suppose c is not prime.

So $c = mn$ where $1 < m < c$, $1 < n < c$.

By above Lemma, $0 = c \cdot 1$

$$= (mn) \cdot (1 1)$$

$$= (m \cdot 1)(n \cdot 1) \quad \text{by } \boxed{\text{Lemma } \star}$$

Since D has no zero divisors,

either $m \cdot 1 = 0$ or $n \cdot 1 = 0$.

By Lemma above, char D equals order of 1.

So char D is less than c, which is a contradiction.

Therefore, c must be prime. □