Math 412

Algebra 2: Electric Boogaloo

- Lord of the Rings $(\mathbb{Z}, +, \cdot)$

<u>def</u>: A ring R is a set w/ 2 binops: $+$ and $\cdot$ that statisfy the following axioms:

- $(R, +)$ is an abelian group
- multiplication is associative
- distributivity laws: $a(b+c) = ab + ac$
  $(a+b)c = ac + bc$

$(a+b)+c = a+(b+c)$
$a+b = b+a$

exists: element 0 s.t $a+0 = 0+a = a$
$\forall a \in R$, $\exists -a$ s.t. $a + -a = 0$

Examples: $(\mathbb{Z}, +, \cdot)$
$(\mathbb{Q}, +, \cdot)$ $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
$(\mathbb{R}, +, \cdot)$
$(\mathbb{C}, +, \cdot)$

<u>def</u> A subset S of a ring R is called a subring if S is a ring with respect to the same bin op

e.g. $\mathbb{Z}$ is a subring of $\mathbb{Q}$

<u>def</u> A ring R is commutative if multiplication is also commutative

Remark: $(R, \cdot)$ is almost never a group since 0 is not invertible :(

Non commutative Ring eg:

$n \times n$ matrices w/ coefficients in some ring R

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \in \mathrm{Mat}_n(R)$$

$$a_{ij} \in R$$

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$$

$$\begin{pmatrix} a_{i1} & \cdots & a_{in} \end{pmatrix} \cdot \begin{pmatrix} b_{ij} \\ \vdots \\ b_{nj} \end{pmatrix} = \left(a_{i1} b_{1j} + \cdots + a_{in} a_{nj} \right)$$

why? find counter example . . .

Rings of Functions

$$F = \{ \text{all functions } f : \mathbb{R} \to \mathbb{R} \}$$
$$(f+g)(x) = f(x) + g(x)$$
$$(f \cdot g)(x) = f(x)\, g(x)$$

Interesting Subrings:

polynomials

Continuous / differentiable / analytic

Def R is a ring w/ unity 1 if $a \cdot 1 = 1 \cdot a \ \forall a \in R$

Example of a ring without unity?

even numbers

Very important Ring: $(\mathbb{Z}_n, +, \cdot)$

remainders mod n

addition and multiplication mod n

Recall $(\mathbb{Z}_n, +)$ is cyclic abelian group with generator 1

1 is also unity for modular multiplication

- Direct Product of Rings:

R, S rings

$$R \times S = \{ (r,s) : r \in R \quad s \in S \}$$
$$(r,s) + (r', s') = (r + r', s + s')$$

$(r,s)(r',s') = (rr', ss')$

Th: 1. $0 \cdot a = a \cdot 0 = 0$

2. $a(-b) = (-a)b = -(ab)$

3. $(-a)(-b) = ab$

Pf

1. $0 \cdot a = (0+0)a = 0 \cdot a + 0 \cdot a$

$\Rightarrow 0 \cdot a + -(0 \cdot a) = 0 \cdot a + 0 \cdot a - (0 \cdot a)$

$\therefore 0 = 0 \cdot a$

$a \cdot 0$ follows same pf

2. $a \cdot -b + a \cdot b = a \cdot (-b + b) = a \cdot 0 = 0$

$\Rightarrow a \cdot -b = -(ab)$

$-a \cdot b$ follows similar pf

3. $(-a)(-b) = -(-a \cdot b) = -(-(ab)) = ab$

$\blacksquare$

def A function $\varphi : R \to S$ (between rings) is a homomorphism

if $\forall a,b \in R$ $\varphi(a+b) = \varphi(a) + \varphi(b)$

and $\varphi(ab) = \varphi(a)\varphi(b)$

an isomorphism is a bijective homomorphism

Examples: $\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}_n$

$\varphi(k) = k \bmod n$ $\quad \varphi(k+l) = k + l \bmod n$

$= \varphi(k) + \varphi(l)$

mod addition

$\varphi(k\ell) = \varphi(k)\varphi(\ell)$

multiply in $\mathbb{Z}$ multiply in $\mathbb{Z}_n$

eg lets say S is a subring of R

the inclusion function $\varphi: S \hookrightarrow R$ is homomorphism

eg $F = \{ f: \mathbb{R} \to \mathbb{R} \}$

we have a homomorphism $F \to \mathbb{R}$ "evaluation"

$$f(x) \longmapsto f(\pi)$$

$$f(x) + g(x) \longmapsto f(\pi) + g(\pi)$$

$$f(x)\,g(x) \longmapsto f(\pi) + g(\pi)$$

are there homomorphisms from $\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$

$\varphi(1) \to (1,2)$ Is it a homomorphism?

no $\varphi(1 \cdot 1) \neq (1,2) \cdot (1,2) = (1,4)$

$\varphi(1) = (a,b)$, $a,b = 0,1$

Kernel of a homomorphism φ is the set of elements x s.t. $\varphi(x) = 0$

Ker φ also forms a subring. Ignoring multiplication, is just the kernel of homomorphism of abelian groups.

Consider ring of integers $\mathbb{Z}$ and $\varphi(n) := 2n$.

φ is bijective, $\varphi(x+y) = 2(x+y) = 2x+2y = \varphi(x)+\varphi(y)$

$\Rightarrow \varphi$ is a isomorphism of abelian groups

but $\varphi(xy) = 2xy \neq \varphi(x)\varphi(y) = 4xy$

Example: Important Isomorphism in Number Theory

Let r and s be coprime integers

$\varphi: \mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s$

$x \bmod rs \to x \bmod r,\ x \bmod s$

(1) φ is a homomorphism

(preserves modular arithmetics)

(2) φ is bijective

$\therefore$ φ is an isomorphism

If we ignore multiplication, this is an isomorphism of cyclic groups.

Surjectivity of $\mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s$ has a name:

given $x \in \mathbb{Z}_r$, $y \in \mathbb{Z}_s$, there exists n s.t.

$$\begin{cases} x = n \bmod r \\ y = n \bmod s \end{cases}$$

AKA Chinese Remainder Theorem

__def__ Suppose R is a ring w/ 1

An element $x \in R$ is called a unit if it has a multiplicative inverse.

__def__ A commutative ring w/ 1 s.t. that every non-zero element is a unit is called a field.

def A ring w/ 1 s.t. every non-zero element is invertible is called a division ring eg. Quarternions

def If a and b are non-zero elements of the ring s.t. $ab = 0$ then a and b are called zero divisors (or division of 0)

eg in $\mathbb{Z}_4$, $2 \cdot 2 = 0$ so 2 is a zero-divisor

Thm let $a \in \mathbb{Z}_n$, $a \neq 0$

then a is a zero-divisor
$\Leftrightarrow \gcd(a, n) \neq 1$

and a is a unit
$\Leftrightarrow \gcd(a, n) = 1$

Corollary $\mathbb{Z}_p$ is a field if p is prime

because $a \in \mathbb{Z}_p$, $a \neq 0$
$\Rightarrow \gcd(a, p) = 1$
$\Rightarrow$ a is invertible by the thm.

Pf Take $a \in \mathbb{Z}_n$, $a \neq 0$, suppose $\gcd(a, n) = d > 1$

$$\underbrace{a \cdot \frac{n}{d} = \frac{a}{d} \cdot n}_{\text{both integers}} \equiv 0 \mod n$$

$a, \frac{n}{d} \in \mathbb{Z}_n$, neither is 0 but $a \cdot \frac{n}{d} = 0$ in $\mathbb{Z}_n$

$\Rightarrow$ a is a zero-divisor

Let's show that a is not a unit. Argue by contradiction. Suppose $a \cdot b = 1$ in $\mathbb{Z}_n$

$$\frac{n}{d} \cdot a \cdot b = \frac{n}{d} \text{ in } \mathbb{Z}_n$$

$$0 = \frac{n}{d} \text{ in } \mathbb{Z}_n$$

This is a contradiction

To summarize, if $\gcd(a, n) > 1$

$\Rightarrow$ a is a zero-divisor and is not a unit

Next, suppose $\gcd(a, n) = 1$

linear combination theorem: gcd of 2 integers is their linear combination.

$$1 = ab + nc$$

Modular: $ab \equiv 1 \mod n$

$\Rightarrow$ a is a unit

It remains to prove that a is not a zero-divisor

By contradiction, suppose $ac = 0$ in $\mathbb{Z}_n$, $c \neq 0$

$$abc = b \cdot 0 = 0 \text{ in } \mathbb{Z}_n$$

$$abc = 1 \cdot c = 0 \text{ in } \mathbb{Z}_n$$

$$c = 0 \text{ in } \mathbb{Z}_n \text{ contradiction}$$

$\Rightarrow$ every non-zero element of $\mathbb{Z}_n$ is either a unit or a zero-divisor depending on whether $\gcd(a, n) = 1$ or not.

<u>def</u> a commutative ring R with 1 and without zero division is called an integral domain.

eg all fields.

(similar arg. $ab=1$ but $ac=0$, then multiply $ac=0$ by b
$abc=0 \Rightarrow 1\cdot c=0$, $c=0$ so a is not a zero-divisor)

$\mathbb{Z}$ is an integral domain but not a field
also: ring of polynomials in 1 variable w/ real coefficients

Solving equations:
$$x^2-5x+6=0$$
Here x can be in some ring R
Solution set depends on R
- $R=\mathbb{R}$ $3,2$
$$x^2-5x+6=(x-3)(x-2)=0$$
$\Rightarrow x=3$ or $x=5$
we use here that R is an integral domain

- $R=\mathbb{Z}_7$
$$(x-3)(x-2)=0$$
$\Rightarrow x=3$ or $x=2$
- $R=\mathbb{Z}_{12}$ - not integral domain
$x=2,3$ are still solutions
Are there other solutions?
$(x-2)(x-3)=0$ but $x\neq 2$ $x=3$
$x=6$ $4\cdot 3=0$ in $\mathbb{Z}_{12}$
$k(k+1)=0$ in $\mathbb{Z}_{12}$
$k=8$ also works

So $X = 2, 3, 6, 11$

<u>def</u> Let R be a ring. The smallest positive integer n, s.t. $n \cdot a = 0$ for every $a \in R$

repeatedly add a, n times

is called the characteristic of R

If no such n exist the characteristic is 0.

eg $\text{char}(\mathbb{Q}) = 0$

$\text{char}(\mathbb{Z}) = p$