Contents

1 LN 18

Groups. M a math structure $\implies$ $Aut(M)$ - auto of M

1.1 Where do rings show up?

The why of rings

1.1.1 Exmple: $(A, +)$ and abelian group

$End(A) = \{f : F : A \to A\}$ $End(A)$ has 2 natural binary operations:

- $+$ $f, g \in$ $End(A)$ TODO
- $*$ $f, g \in$ $End(A)$ then $f \cdot g$ $:= f \circ g$ This is still a homomorphism. $(End(A), \cdot)$ is associative and id_A is the identity.
- Check distributivity! $(End(A), +, \cdot)$ is a ring.

1.1.2 Example: What is we look at $End(\mathbb{Z}, +)$?

All $f : \mathbb{Z} \to \mathbb{Z}$ and determined by where 1 goes. Say $f(1) = n$ and $g(1) = m$, what is $g(f(1))$?

So $End(\mathbb{Z}, +) = (\mathbb{Z}, +\cdot)$.

1.1.3 Example: $V = \mathbb{C}^n$

V is complex n-space and look $\mathbb{R}$, the set of all linear tranformations $F : V \to V$

- $+$ on $\mathbb{R}$ $f, g : V \to V$ on linear transformations, so is $f + g$
- $\cdot$ on $\mathbb{R}$ is just composition $f \cdot g = f \circ g$.

Check that $(R, +, \cdot)$ is a ring with 1 - 1 $= id_V$
This is $M_n(\mathbb{C})$ - $n \times n$ complex matrices.

1.1.4 Subring

If R is a ring and $S \subseteq R$, then we say S is a subring of R if S with $+$ and $\cdot$ from R restricted to S is a ring

- Example $(\mathbb{Z}, +, \cdot)$ Then $n\mathbb{Z} = \{nm : m \in \mathbb{Z}\} \subseteq \mathbb{Z}$is a subring but noice if $n \neq \pm 1$ then $n\mathbb{Z}$ does not have a 1.

If R, S TODO

1.1.5 Ring homomorphism

If \$$\phi :$ R $\to$ S\$is a ring homomorphism then $ker(\phi) = \{a \in R : \phi(a) = 0\}$
Fact: \$ker(R)\$is closed under + and if $a \in\ ker(\phi),\ r \in R$ then $ar, ra \in ker(\phi)$

1.2 Ideals

If R is a ring and $I \subseteq R$ then I is an ideal if $(I, +)$ is an abelian group and $\forall a \in I, r \in R, ar, ra \in I$
Notice TODO

- Example: What are ideals of $(\mathbb{Z}, +, \cdot)$? $\{0\}$, $p\mathbb{Z}$, $n\mathbb{Z}$ $\forall n \in \mathbb{Z}$ (this is general ideal in $\mathbb{Z}$)

1.2.1 Why do we care about ideals?

We want to make sense of quotients!

Given $BI \subseteq R$, R some ring and I an ideal. we want to define $\dfrac{R}{I}$ is a ring.
TODO

1.2.2 How do we define $(r+I)(s+I)$ for $r, s \in R$?

Define $(r+I)(s+I) = rs + I$. we need to se that this is well-defined. If $r + I = r' + I$, ie $r - r' \in I$ then $(r - r')s \in I$ because I is an ideal. $\because I$ is an ideal, so $rs + I = r's + I$.

We do something similar for s so multiplication is well-defined.

- Check: $\dfrac{R}{I}$is a ring with these operations.
    - Example $\mathbb{Z}$ has $n\mathbb{Z}$ as ideals for $n \in \mathbb{Z}$ What is $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ as a ring ?

      This is arithmatic mod n.

      1st Isomorphism Theorem: If $\phi : R \to S$ is a ring homomorphism then $\dfrac{R}{ker(\phi)} \cong Im(\phi) \subseteq S$.

      Notice: Every ideal is th kernel of some ring homomorphisms. $\phi : R \to \dfrac{R}{I}, i \mapsto r + I$, then $ker(\phi) = I$.

TODO: hard to draw the diagram Rings $\to +, \cdot$, satisfying ... Rings with identity Rings without identity. Commutative Non-commutative Integral domain Division ring (multi-inverse of non-zero elements (No 0 divisors but not nes. commutative) ie if $ab = 0$ then $a = 0$ or $b = 0$) Fields: division ring and integral domain (every non-zero elements has a multiplicative inverse)

Judson, pg 192 quaternions TODO