Math 5286 Spring 2019 Vic Reiner

1/23/2019

Honors Fundamental Structures of Algebra II

- Go through syllabus items really quickly
- Set office hours, e.g. MF 9:05am–9:55am & Tu 12:20pm–1:10pm ?

Last semester – lots of groups and matrices over fields, linear algebra, vector spaces

This semester – we'll learn more about fields, matrices and abelian groups

if we start studying rings, particularly polynomial rings

$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$

$a_i \in \mathbb{F}$ some field

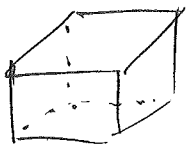
For example, just a little bit of ring theory and polynomials (Chaps 11 & 12) will let us show

- all finite fields $\mathbb{F}$ must have cardinality $|\mathbb{F}| = p^r$ a prime power, and their multiplicative group $\mathbb{F}^\times := (\mathbb{F} - \{0\}, \times)$ is cyclic i.e. isomorphic to $(\mathbb{Z}/(p^r-1)\mathbb{Z}, +)$
- using (§15.5) only usual compass/straightedge constructions one can never

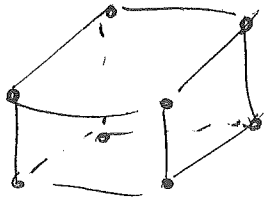
- "square" a circle, i.e. given a circle

produce the sidelength for a square with same area

- "duplicate" a cube, i.e. given a cube



produce the sidelength for a cube with twice the volume



- then some more field theory (Galois theory (Chap. 16)) lets us understand using group theory (!?) why quadratic formula $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$ for $ax^2+bx+c=0$

ought to have cubic (deg 3), quartic (deg 4) versions, but not quintic (deg 5).

- then some theory of modules over rings (Chap. 14)
↖ like vector spaces over fields

lets us understand why finite abelian groups are always of the form $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \dots \times \mathbb{Z}/n_\ell\mathbb{Z}$

and why Jordan canonical form for matrices $A \in \mathbb{C}^{n\times n}$ should exist

---

We plan on skipping Artin's Chap. 13, for lack of time (not interest!)

So let's get to it ...

Chap. 11 Rings

§11.1, 11.2 Definition & examples

DEF'N: (11.1.3) A ring R is a set with two binary operations $+, \times$ (so $R \times R \to R$, $(a,b) \mapsto a+b$; $R \times R \to R$, $(a,b) \mapsto a \cdot b$)

satisfying these properties:

(a) $(R,+)$ is an abelian group (i.e. $+$ is associative, commutative)
with additive identity called $0 \in R$ ($0+a = a+0 = a$ $\forall a \in R$)
$\exists -a \in R$ with $(-a)+a = 0 = a+(-a)$

(b) $(R,\times)$ is associative ($(ab)c = a(bc)$), commutative ($a \cdot b = b \cdot a$)
and has a multiplicative identity called $1 \in R$ (so $1 \cdot a = a \cdot 1 = a$)

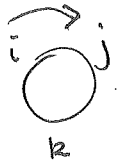
(c) $\times$ distributes over $+$: $a(b+c) = ab + ac$
$(b+c)a = ba + ca$

REMARKS:

(1) In some books, this would be called a commutative ring, and they would not insist that $\times$ be commutative i.e. $ab \neq ba$ sometimes

e.g. $\mathbb{H}$ = Hamilton's quaternions is a noncommutative ring

$= \{a+bi+cj+dk : a,b,c,d \in \mathbb{R}\}$



$ij = k = -ji$
$jk = i = -kj$
$ki = j = -ik$

In our book, all rings are commutative!

---

(2) In some books, our rings would be called rings with 1, and if $(R,\times)$ had no multiplicative identity, it would be called a ring without 1 or a "rng" (!)

---

(3) Our (commutative) rings (with 1) might not be fields only because we don't insist that every $a \in R - \{0\}$ has a (2-sided) multiplicative inverse a^{-1} i.e. $a \cdot a^{-1} = 1 = a^{-1} \cdot a$ ($\Rightarrow$ a^{-1} is unique: if $ab = 1$ and $ca = 1$ then cab "$c(ab)$" "$(ca)b$" "$1 \cdot b$" "b" "$c \cdot 1$" "c")

i.e. $R^\times := \{a \in R : \exists$ a mult. inverse for a in $R\}$

= the group of units of R

might be strictly smaller than $R - \{0\}$

(for a field $\mathbb{F}$ $\quad \mathbb{F}^\times = \mathbb{F} - \{0\}$)

---

(4) Possibly $1 = 0$, but then this forces $R = \{0\}$ the zero ring, since $a = 1 \cdot a = 0 \cdot a = 0$ $\forall a \in R$ (EXERCISE from Fall semester or see PROP 11.1.5)

---

(5) Obvious notion of subring $R' \subset R$, a subset containing $0, 1$ and closed under $+, \times$