10/7

Rings §3.1

The number systems we are used to (like $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \ldots$) have two fundamental operations: addition $+$, and multiplication $\cdot$. A ring is an abstract algebraic system that captures the way $+$ and $\cdot$ interact in number systems. The definition of ring builds on that of abelian group, and much of what we have learned about groups will continue to apply to rings, which are our focus of study for the 2nd half of the semester.

Def'n A ring is a set R with two binary operations $+: R\times R \to R$ and $\cdot: R\times R \to R$ satisfying the following axioms:

- addition is associative: $(a+b)+c = a+(b+c)$
- there is an additive identity 0: $a+0=0+a=a$
- there are additive inverses: $a+(-a)=(-a)+a=0$
- addition is commutative: $a+b=b+a$

$\Rightarrow$ So $(R,+)$ is an abelian group

- multiplication is associative: $(a\cdot b)\cdot c = a\cdot(b\cdot c)$
- there is a multiplicative identity 1: $a\cdot 1 = 1\cdot a = a$

$\Rightarrow$ So $(R,\cdot)$ is a monoid

- multiplication distributes over addition:
  $$a\cdot(b+c) = a\cdot b + a\cdot c \quad \text{and} \quad (b+c)\cdot a = b\cdot a + c\cdot a$$

WARNING: In the textbook, they do not assume that rings have a 1 (multiplicative identity), and call a ring unital or "with unity", if it does. We will always assume rings have a 1. Interesting examples do.

There is a nested sequence of classes of rings

rings $\subseteq$ commutative rings $\subseteq$ domains $\subseteq$ fields

that behave more and more like the number systems we know.

Def'n A ring R is called commutative if the multiplication is commutative: $a\cdot b = b\cdot a$.

WARNING Addition in a ring (even a "noncommutative" ring) is always commutative! But multiplication might not be.

We now give many examples of rings.

E.g: The first example of a ring to have in mind is $R = \mathbb{Z}$, the integers with their usual addition & multiplication. This is a commutative ring.

E.g. For any integer $n \geq 1$, we can take $R = \mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$ with addition and multiplication modulo n. This is a finite commutative ring.

E.g. Let R be any commutative ring, e.g. $R = \mathbb{Z}$. For $n \geq 1$, we use $M_n(R)$ to denote the ring of $n \times n$ matrices with entries in R, with addition componentwise, and with multiplication the multiplication of matrices you know from linear algebra. This is a noncommutative ring:

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \text{ but } \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

E.g. Let R be any commutative ring, e.g. $R = \mathbb{Z}$ and let G be a group. The group ring (or group algebra) $R[G]$ has as its elements formal finite R-linear combinations of elts. of G: i.e., expressions of the form $\sum_{g \in G} r_g\, g$ (where $r_g = 0$ for all but finitely many of the $g \in G$). Addition is coordinatewise: $\sum_{g \in G} r_g\, g + \sum_{g \in G} r_g'\, g = \sum_{g \in G} (r_g + r_g')\, g$.

For multiplication: $\left(\sum_{g \in G} r_g\, g\right) \cdot \left(\sum_{g \in G} r_g'\, g\right) = \sum_{g, g' \in G} (r_g \cdot r_{g'}') (g \cdot g')$

where $(g \cdot g') \in G$ is using the group multiplication.

This group algebra is commutative iff the group G is commutative. Let's see a

Concrete example: consider $\mathbb{Z}[S_3]$, group algebra of symmetric group S_3.

Then $(e + 2\cdot(1,2))\cdot(-3e + (1,3)) =$

$-3\,e\cdot e + e\cdot(1,3) - 6\,(1,2)\cdot e + 2\underbrace{(1,2)\cdot(1,3)}_{=(1,3,2)} = -3e + (1,3) - 6(1,2) + 2\,(1,3,2)$

Can multiplication give a group structure on a ring R?
No, inverse of zero never exists* because of following:

Prop: In any ring R, $a\cdot 0 = 0\cdot a = 0$ for all $a \in R$.

Pf: $a\cdot 0 = a\cdot(0+0) = a\cdot 0 + a\cdot 0 \Rightarrow 0 = a\cdot 0$. (subtract $a\cdot 0$ from both sides) $\boxtimes$

Rmk: * technically in the trivial ring R with one element $0=1$ we have that 0 is multiplicatively invertible.
But in any nontrivial ring R, $0 \neq 1$, so 0 is not multiplicatively invertible.

Def'n Let R be a ring. An $a \in R$ is called a left (resp. right) zero divisor if $\exists\, x \in R$ such that $ax = 0$ (resp. $xa = 0$).

E.g. 0 is always a zero divisor in every ring.

E.g. 2 is a zero divisor in $\mathbb{Z}/6\mathbb{Z}$ since $2\cdot 3 = 6 = 0$.

E.g. $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in M_2(\mathbb{Z})$ is a left and right zero divisor, since $A^2 = 0$.

Def'n A commutative ring R is called an integral domain, or just domain, if it has no nonzero zero divisors.

E.g. We saw that $\mathbb{Z}/6\mathbb{Z}$ is not a domain.

E.g. $\mathbb{Z}$ is a domain. It is the prototypical example of one.

Exercise: Show that $\mathbb{Z}/p\mathbb{Z}$ for p a prime is a domain. In fact, it is a finite field, which we now explain...

Def'n An element $a \in R$, for R a ring, is called a unit if it is multiplicatively invertible, i.e. $\exists b \in R$ s.t. $ab = ba = 1$.
We use $R^{\times}$ to denote the units of R, which forms a group under $\cdot$.

E.g. $\mathbb{Z}^{\times} = \{-1, 1\}$, while $(\mathbb{Z}/p\mathbb{Z})^{\times} = \{1, 2, \ldots, p-1\}$ for p prime.

Prop. If $a \in R$ is a unit, then it is not a zero divisor.

Pf. $a \cdot x = 0 \Rightarrow a^{-1} \cdot a \cdot x = a^{-1} \cdot 0 \Rightarrow x = 0$. $\blacksquare$

Def'n A commutative ring R is called a field if every nonzero element is a unit, i.e. if $R^{\times} = R \setminus \{0\}$.
Notice that a field is a domain, thanks to the last proposition.

Eg. $\mathbb{Z}$ is not a field. But the rational numbers $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$ are a field. Similarly the real numbers $\mathbb{R}$ and complex numbers $\mathbb{C}$ are fields.

Def'n A (noncommutative) ring R is called a division ring or a skew field if every nonzero element is a unit.

Skew fields are weirder than fields, but here is an important example:

E.g. The skew field $\mathbb{H}$ of quaternions (where H = W.R. Hamilton, their discoverer) has elements of the form $p = a + b\bar{i} + c\bar{j} + d\bar{k}$ where $a, b, c, d \in \mathbb{R}$ are real numbers, and $\bar{i}, \bar{j}, \bar{k}$ are formal symbols satisfying the identities $\bar{i}^2 = \bar{j}^2 = \bar{k}^2 = \bar{i}\bar{j}\bar{k} = -1$ (compare to the complex numbers $z = a + b\bar{i}$).
For instance, $(1+\bar{i})(1+\bar{j}) = 1 + \bar{i} + \bar{j} + \bar{i}\bar{j} = 1 + \bar{i} + \bar{j} + \bar{k}$,
where $\bar{i}\bar{j} = \bar{k}$ because $\bar{i}\bar{j}\bar{k} = -1 \Rightarrow \bar{i}\bar{j}\bar{k}^2 = -\bar{k} \Rightarrow -\bar{i}\bar{j} = -\bar{k}$.

Ring homomorphisms § 3.1

Like we saw with groups, for rings as well studying the structure-preserving maps between them is very important.

Def'n Let R and S be rings. A homomorphism $\varphi : R \to S$ is a map such that:
- $\varphi(a+b) = \varphi(a) + \varphi(b) \quad \forall a,b \in R$
- $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \quad \forall a,b \in R$
- $\varphi(1_R) =$ [redacted] 1_S (sends 1 to 1)

Note: That $\varphi(0_R) = 0_S$ follows from the above, so is not needed!

WARNING: Again since the textbook does not assume rings are unital, it does not assume ring homo.'s preserve 1. But we always will!

Def'n For $\varphi : R \to S$ a ring homo., we call φ a monomorphism if it is injective, an epimorphism if it is surjective, & an isomorphism if both.

E.g. The inclusions $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{H}$ give us canonical monomorphisms from rings on left to rings on right.

E.g. For each $n \geq 1$, $\exists$ a canonical epimorphism $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ given by $\varphi(a) = a \bmod n$.

E.g. A monomorphism $\varphi : M_n(R) \to M_{n+1}(R)$ is given by $\varphi(A) = \begin{bmatrix} A & \vdots \\ & 0 \\ 0 \cdots 0 & 1 \end{bmatrix}$ (put A in upper left corner).

Exercise: Show that a homomorphism $\varphi : G \to H$ between two groups induces a homo. $\varphi : R[G] \to R[H]$ of their group algebras.

Def'n Let $\varphi : R \to S$ be a ring homo. The image of φ is $\mathrm{im}(\varphi) = \{\varphi(a) : a \in R\} \subseteq S$ and the kernel of φ is $\mathrm{Ker}(\varphi) = \{a \in R : \varphi(a) = 0\} \subseteq R$, just like with groups.

Again, images and kernels lead to sub- and quotient structures...