10/7

Rings §3.1

The number systems we are used to (like $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \dots$) 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.

<u>Def'n</u> 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 $\supseteq$ commutative rings $\supseteq$ domains $\supseteq$ fields

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

<u>Def'n</u> 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) ☒

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 $\exists\, x \in R$, $x \neq 0$ 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 $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, \dots, p-1\}$ for p prime.

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

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

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 $\bar{i}\bar{j}\bar{k} = -1 \Rightarrow \bar{i}\bar{j}\bar{k}^2 = -\bar{k} \Rightarrow -\bar{i}\bar{j} = -\bar{k}$.

10/9

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:
- $\varphi(a+b) = \varphi(a) + \varphi(b) \quad \forall a,b \in R$
- $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \quad \forall a,b \in R$
- $\varphi(1_R) = 1_S$ (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 $\varphi(A) = \begin{bmatrix} A & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ 0 \cdots 0 & 1 \end{bmatrix}$ (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 $\operatorname{im}(\varphi) = \{\varphi(a) : a \in R\} \subseteq S$ and the kernel of φ is $\operatorname{Ker}(\varphi) = \{a \in R : \varphi(a) = 0\} \subseteq R$, just like with groups.

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

Ideals §3.2

<u>Def'n</u> Let R be a ring. A <u>subring</u> $S \subseteq R$ is a subset such that: • $0 \in S$, • $a,b \in S \Rightarrow a+b \in S$, • $a \in S \Rightarrow -a \in S$
(so S is a subgroup of $(R,+)$)
• $1 \in S$, • $a,b \in S \Rightarrow ab \in S$
(so S is a submonoid of $(R,\cdot)$).

We want to take quotient of rings. Just like we saw with groups (where <u>normal</u> subgroups were key) need different thing than subrings:

<u>Def'n</u> Let R be a ring. A <u>left</u> (resp. <u>right</u>) <u>ideal</u> of R is a subset $I \subseteq R$ s.t.: • $0 \in I$, • $a,b \in I \Rightarrow a+b \in I$, • $a \in I \Rightarrow -a \in I$
(so I is a subgroup of $(R,+)$)
• $a \in R$, $x \in I \Rightarrow ax \in I$ (resp. $xa \in I$).

An <u>ideal</u> (or <u>two-sided</u> <u>ideal</u>) is $I \subseteq R$ that is both a left & right ideal.

<u>E.g.</u> Since $1 \in \mathbb{Z}$ generates $\mathbb{Z}$, $\mathbb{Z}$ has no proper subrings. But for each $n \geq 1$, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

<u>E.g.</u> $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{H}$ as subrings. But a field K (like $\mathbb{Q}, \mathbb{R}, \mathbb{C}$) has no nontrivial ($\neq 0, K$) ideals.

<u>WARNING</u>: Since the book does not assume $1 \in R$, it does not assume $1 \in S$ for subrings, but <u>we</u> <u>will</u>. So note a proper ideal $I \subsetneq R$ is <u>never</u> a subring, since $1 \notin I$.

<u>Prop.</u> Let $\varphi: R \to S$. Then:
i) $\mathrm{im}(\varphi)$ is a subring of S
ii) $\ker(\varphi)$ is an ideal of R.

<u>Pf</u>: Straightforward, same as for groups. ∎

Ideal theory is best behaved for <u>commutative</u> rings R, but good also to have in mind some noncommutative examples.

<u>E.g.</u> For any $k \leq n$, $M_k(R)$ is a subring of $M_n(R)$ (by putting $k \times k$ matrix in upper-left corner).
For any ideal $I \subseteq R$, $M_n(I)$ is an ideal of $M_n(R)$.

<u>E.g.</u> For a subgroup $H \subseteq G$, $R[H]$ is a subring of $R[G]$.
For any ideal $I \subseteq R$, $I[G]$ is an ideal of $R[G]$.

Given an ideal $I \subseteq R$, we can consider the cosets $a + I = \{a + x : x \in I\}$ for $a \in R$, the set of which we denote R/I.
Because I is a subgroup of the abelian group $(R, +)$, R/I is an abelian group under the usual addition:

$$(a+I) + (b+I) = (a+b) + I.$$

<u>Prop.</u> The quotient R/I for $I \subseteq R$ an ideal has the structure of a ring, with multiplication given by $(a+I) \cdot (b+I) = ab + I$.

<u>Pf.</u> See book. For noncommutative R it is important that I be a (two-sided) ideal here. ∎

<u>E.g.</u> For each $n \geq 1$, $\mathbb{Z}/n\mathbb{Z}$ the quotient ring is exactly $\{0, 1, \ldots, n-1\}$ with multiplication and addition modulo n, as we have seen.

<u>E.g.</u> 0 is an ideal of any R, and $R/0 = R$.

Rmk: There are versions of all the isomorphism theorems we saw for quotient groups that hold for quotient rings too... see the book.

Certain families of ideals are especially important

Def'n An ideal $I \subseteq R$ of a (not necessarily commutative) ring R is called prime if $AB \subseteq I \Rightarrow A \subseteq I$ or $B \subseteq I$ for all ideals A, B, where $AB = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n : a_i \in A, b_i \in B\}$.

The definition of prime ideal is easier if R is commutative:

Prop. An ideal $I \subseteq R$ of a commutative ring R is prime if $\forall a, b \in R$, $ab \in I \Rightarrow a \in I$ or $b \in I$. pf: See book.

E.g. $p\mathbb{Z}$ for p a prime is a prime ideal of $\mathbb{Z}$, and $0\mathbb{Z}$ is also a prime ideal. (these are all)

Def'n An ideal $I \subseteq R$ of a ring R is called maximal if it is not contained in any proper ($\neq R$) ideal.

Prop. In a commutative ring R, every max'l ideal is prime.

E.g. $p\mathbb{Z}$ for p prime are the maximal ideals of $\mathbb{Z}$, but note $0\mathbb{Z} = 0$ is prime although it is not maximal.

The conditions of prime and maximal imply important properties of the corresponding quotient rings.

Prop. Let R be a commutative ring and $I \subseteq R$ an ideal. Then i) I is prime $\Leftrightarrow R/I$ is a domain

ii) I is maximal $\Leftrightarrow R/I$ is a field.

E.g. $\mathbb{Z}/p\mathbb{Z}$ for p a prime is a finite field, as we have seen, while $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$ is a domain, which we have also seen.

Exercise: prove the above propositions! (or see book...)

//

10/16

Factorization in Commutative Rings § 3.3

The fundamental theorem of arithmetic says that every positive integer n can be written uniquely as $n = p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell}$, a product of prime numbers. We will explore extensions of this property to other commutative rings beyond $\mathbb{Z}$.

Note: Today all rings R considered will be commutative!

Def'n Let R be a commutative ring, and $a, b \in R$ elements. We say that a divides b, written $a | b$, if $\exists\, c \in R$ such that $ac = b$. We say that a and b are associates if $a | b$ and $b | a$.

Prop. 1) If $a = ub$ where $u \in R$ is a unit, then a & b are associates.

2) If R is an integral domain, then conversely for any two associates $a, b \in R$ we have $a = ub$ with u a unit of R.

Pf: 1) obvious. 2) Suppose $b \neq 0$ by symmetry. Then

$a = cb$ and $da = b$ means $dcb = b \Rightarrow (dc - 1)b = 0$

and since R is a domain and $b \neq 0 \Rightarrow dc - 1 = 0$ i.e. $d = c^{-1}$! ∎

Rmk: We need notion of associates to make sense of the "uniqueness" in the statement of fund. thm. of arithmetic. Think: multiplying by -1.

Def'n An element $c \in R$ is called irreducible if c is a nonzero nonunit and $c = ab \Rightarrow a$ or b is a unit.

$p \in R$ is called prime if p is a nonzero nonunit and $p | ab \Rightarrow p | a$ or $p | b$.

Rmk: Compare to the definition of prime ideal. In fact, we can make a direct connection between these notions... From now on let's assume R is an integral domain.

Def'n Given $a_1, \dots, a_n \in R$, we use $\langle a_1, \dots, a_n \rangle$ or $(a_1, \dots, a_n)$ to denote the ideal generated by $a_1, \dots, a_n$, the smallest ideal $I \subseteq R$ containing all a_i. We say an ideal $I \subseteq R$ is principal if $I = (a) = \{xa : x \in R\}$ for a single element $a \in R$.

Prop. $p \in R$ is prime $\iff$ (p) is a nonzero prime ideal of R.

What about the relationship between prime & irreducible?

Prop: Every prime element of R is irreducible.

Rmk: Converse is not true in general for integral domains! On your next HW you will show an example. But converse is true in many nice domains...

Def'n An integral domain R is called a unique factorization domain (UFD) if every nonzero nonunit $a \in R$ can be written as $a = c_1 c_2 \cdots c_n$ with $c_i \in R$ irreducible, and if we have two such expressions $a = c_1 \cdots c_n$ and $a = d_1 \cdots d_m$ then $n = m$ and there is a permutation σ of $\{1, 2, \dots, n\}$ such that c_i and $d_{\sigma(i)}$ are associates for all i.

- A UFD is a domain where the analog of the fundamental theorem of arithmetic holds, like $\mathbb{Z}$. The uniqueness is up to associates because we can always multiply by units.

Rmk: Notice that fields are trivially UFD's: factoring is not interesting for units, so we ignore them.

- To study UFD's, we will consider other related classes of commutative rings, giving us inclusions:

integral domain $\supseteq$ UFD $\supseteq$ principal ideal domain (PID) $\supseteq$ Euclidean domain $\supseteq$ fields

Again, everything here is trivial for fields, so think of $R = \mathbb{Z}$ instead.

Def'n An integral domain R is called a <u>principal</u> <u>ideal</u> <u>domain</u> (<u>PID</u>) if every proper ($\neq R$) ideal is principal.

<u>E.g.</u> $\mathbb{Z}$ is a PID since all proper ideals are $n\mathbb{Z} = (n)$ for $n=0$ or $n \geq 2$.

<u>Thm</u> If R is a PID then it is a UFD.

<u>Pf idea</u>: The proof is slightly technical and you can see the book for complete details, but the basic idea is this. We start with some $a \in R$ that we want to factor into irreducibles. We can assume a itself is not yet irreducible. Then (a) ~~belongs~~ is properly contained in some maximal (proper) ideal, which because R is a PID must be of the form (c) for some $c \in R$ that is irreducible (by maximality). So then $c \mid a$, and we can repeat the argument on $b = \frac{a}{c}$ to build up a factorization ~~of~~ of a into irreducibles, unique up to associates. That the process terminates in a finite number of steps relies on an "ascending chain condition," which is one subtlety. $\boxtimes$

Okay, but how to show a commutative ring is a PID?

Def'n An integral domain R is called a <u>Euclidean domain</u> if there is some function $\varphi: R \setminus \{0\} \to \{0, 1, 2, \ldots\}$ s.t.

i) for all $a, b \in R \setminus \{0\}$, $\varphi(a) \leq \varphi(ab)$

ii) for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that $a = qb + r$ with $r = 0$ or $\varphi(r) < \varphi(b)$.

A Euclidean domain is a ring which has something like the <u>Euclidean algorithm</u> for <u>division</u>. In the definition above, think $q = \frac{a}{b}$ is "quotient" and $r =$ "remainder".

<u>E.g.</u> $R = \mathbb{Z}$ is a Euclidean domain with φ being $\varphi(x) = |x|$ (absolute value).

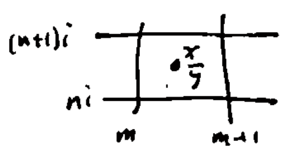
Thm If R is a Euclidean domain then it is a PID (& hence a UFD).

Pf: Let I be a nonzero ideal in R, and pick $a \in I$ such that it minimizes $\varphi(x)$ for all $x \in I \setminus \{0\}$. Then we claim $I = (a)$. Indeed, let $b \in I$. Then $b = qa + r$ for $r = 0$ or $\varphi(r) < \varphi(a)$. But since $a \in I$, $qa \in I$, hence $r \in I$, and if $\varphi(r) < \varphi(a)$ that would contradict our assumption on a. So $r = 0$ and indeed every $b \in I$ is a multiple of a, so $I = (a)$. $\boxtimes$

Given this thm, it is interesting to find more examples of Euclidean domains...

E.g. If $R = K[x]$ is the polynomial ring over a field K, then R is a Euclidean domain thanks to the polynomial long division algorithm. We'll discuss this next class.

E.g. Let $R = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ where $i = \sqrt{-1}$, the ring of Gaussian integers. We can define $\varphi(a+bi) = a^2 + b^2$, and then for $x, y \in R$ we can check that $x = yq + r$ works if we pick q to be the "closest" Gaussian integer to $\frac{x}{y} \in \mathbb{C}$.



$\Rightarrow$ $q = m + ni$ when $\frac{x}{y}$ lies in this square.

E.g. For a counter-example, let $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{5} : a, b \in \mathbb{Z}\}$. On the homework you will show that this is not a UFD, hence not a PID nor a Euclidean domain. The idea is that $2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$ shows that these ~~numbers~~ elements are not prime, although they are irreducible (and in a UFD, $x \in R$ is irreducible $\Leftrightarrow$ x is prime).

10/21

Polynomial rings and formal power series rings §3.5

A very important family of commutative rings are the polynomial rings (in fact, "commutative algebra"/"algebraic geometry" study those!).

Def'n Let R be a commutative ring. The polynomial ring $R[x]$ has elements formal expressions of the form

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad \text{for } a_i \in R, \quad n \geq 0$$

with coefficientwise addition:

$$\sum_{i=0}^{n} a_i x^i + \sum_{j=0}^{m} b_j x^j = \sum_{i=0}^{\max(n,m)} (a_i + b_i) x^i \quad (\text{with } a_i = 0 = b_j \text{ if } i \geq n \text{ or } j \geq m)$$

and multiplication by convolution:

$$\left(\sum_{i=0}^{n} a_i x^i\right) \cdot \left(\sum_{j=0}^{m} b_j x^j\right) = \sum_{k=0}^{n \cdot m} \left(\sum_{i+j=k} a_i b_j\right) x^k .$$

This is just the usual multiplication of polynomials we know:

e.g. $(3x^2 - 4x + 1) \cdot (-2x^2 + x + 5) = -6x^4 + 11x^3 + 9x^2 - 19x + 5.$

Technically we can identify the polynomial $f(x) = \sum_{i=0}^{n} a_i x^n$ with the infinite sequence $(a_0, a_1, a_2, \dots)$ of coefficients $a_i \in R$, where $a_i = 0$ for all but finitely many i. Recall that the biggest i such that $a_i \neq 0$ is called the degree of $f(x)$ (and we either let $\deg(0) = -\infty$ or leave it undefined).

Prop: For any commutative ring R, $R[x]$ is a commutative ring, with a canonical inclusion $\varphi: R \to R[x]$.
If R is an integral domain, then so is $R[x]$, in particular we have $\deg(f \cdot g) = \deg(f) \cdot \deg(g)$ in this case. Pf: Straightforward exercise, see book. ☒

Note: Although we often think of polynomials as functions, the elements of $R[x]$ are just formal expressions, not functions.

E.g., with $R = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ (field with two elements), notice that $f(x) = x$ and $g(x) = x^2$ define the same function $\mathbb{F}_2 \to \mathbb{F}_2$ (since $f(0) = g(0) = 0$ and $f(1) = g(1) = 1$) but they are not considered the same polynomials.

All polynomial rings are infinite (even over finite rings)!

Nevertheless, the idea of viewing a polynomial as a fn, is useful.

Prop: Given any $s \in R$, there is an evaluation homomorphism $\varphi_s : R[x] \to R$ given by $\varphi_s(f(x)) = f(s) = \sum_{i=0}^{n} a_i (s)^i$.

Pf: Straightforward, but note requires R to be commutative! ∎

Note: Given a polynomial $f(x)$, it's important to know what coefficient ring R is where $f(x) \in R[x]$ lives, in order to understand its algebraic properties.

E.g. $f(x) = x^2 - 2$ is irreducible when viewed as an elt. of $\mathbb{Q}[x]$, but $f(x) = (x^2-2) = (x+\sqrt{2})(x-\sqrt{2}) \in \mathbb{R}[x]$. Similarly, x^2+1 is irreducible in $\mathbb{R}[x]$, but in $\mathbb{C}[x]$ have $(x^2+1) = (x+i)(x-i)$.

Can also define multivariate polynomial ring $R[x_1, \ldots, x_n]$ in the natural way, but since we defined $R[x]$ for any polynomial ring (including R = a polynomial ring) it's also easy to just define this iteratively.

Def'n: $R[x,y] = (R[x])[y]$ where x and y are both indeterminates. Elts of $R[x,y]$ are things like $f(x,y) = x^2 - xy + y^3 - 4$. Similarly for $R[x_1, \ldots, x_n]$, polynomial ring with n indeterminates.

§3.6

Factorization in polynomial rings is an important topic.

Theorem Let k be a field. Then $k[x]$, the polynomial ring, is a Euclidean domain, hence a PID, hence a UFD.

Pf. We define the Euclidean norm function to be $\varphi(f) = \deg(f)$ for all $f \in k[x] \setminus \{0\}$. Then the polynomial long division algorithm that you learned in grade school certifies that we can always write $f(x) = q(x) \cdot g(x) + r(x)$ where $\deg(r(x)) < \deg(g(x))$, so indeed we have a Euclidean domain. ☒

Rmk: Recall that polynomial division requires dividing coefficients, explaining why we need a field k here.

$$\begin{array}{r|l} & \tfrac{1}{2}x + 1.25 \\ 2x+1 & x^2 + 3x - 7 \\ & x^2 + \tfrac{1}{2}x \\ \hline & 2.5x - 7 \\ & 2.5x + 1.25 \\ \hline & -8.25 \end{array}$$

$\Rightarrow x^2 + 3x - 7 = (\tfrac{1}{2}x + 1.25)(2x+1) - 8.25$

Note: If R is not a field, then $R[x]$ will not be a PID.

E.g. on your next HW you will show $I = \langle 2, x \rangle \subseteq \mathbb{Z}[x]$ is not a principal ideal in $\mathbb{Z}[x]$.

Nevertheless, we do have the following:

Thm If R is a UFD, then $R[x]$ is also a UFD.

The proof is beyond what we'll be able to cover today, see the book. But the key lemma is this:

Lemma (Gauss's Lemma) Let R be a UFD and K its field of fractions. Then $f(x) \in R[x]$ is irreducible if and only if $f(x) \in K[x]$ is irreducible, and $f(x) \in R[x]$ is primitive.

Here $f(x) = \sum_{i=0}^{n} a_i x^i$ is primitive if $\gcd(a_0, \dots, a_n) = 1$, to rule out e.g. $2x + 4 = 2(x+2) \in \mathbb{Z}[x]$. Meanwhile the field of fractions construction we will learn next class, but e.g. field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$.

The formal power series ring $R[[x]]$ extends poly. ring $R[x]$.

Def'n Let R be a commutative ring. The ring of formal power series $R[[x]]$ has elements formal expressions
$$f(x) = \sum_{i=0}^{\infty} a_i x^i, \quad a_i \in R$$
with the same coefficient wise addition and multiplication by convolution as in the polynomial ring.

Prop. There is a natural inclusion $i: R[x] \hookrightarrow R[[x]]$.

But again, note that properties of $f(x)$ depend on whether we view it as in $R[x]$ or in $R[[x]]$.

E.g.: $(1-x) \in \mathbb{Z}[x]$ is not a unit, but in $\mathbb{Z}[[x]]$ we have $\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots = \sum_{i=0}^{\infty} x^i$

since $(1-x)\cdot(1+x+x^2+x^3+\cdots) = \begin{array}{l} 1 + x + x^2 + \cdots \\ \quad - x - x^2 - \cdots \end{array} = 1.$ ✓

In $\mathbb{C}[[x]]$ we can make sense of Taylor series

i.e. $e^x = 1 + x + \frac{1}{2!}x^2 + \frac{1}{3!}x^3 + \cdots = \sum_{k=0}^{\infty} \frac{1}{k!} x^k$.

But again, we don't view elements of $\mathbb{C}[[x]]$ as functions, in particular, they don't need to converge anywhere!

Rmk: Can define a metric on $R[x]$ by ~~[illegible]~~ defining the distance between $f, g \in R[x]$ to be $2^{-\deg(f-g)}$. Then $R[[x]]$ is the completion of $R[x]$ with respect to this metric, and enjoys some universal/categorical properties.

Rmk: The formal power series ring $\mathbb{C}[[x]]$ in enumerative combinatorics as a place where generating functions of counting sequences can live!