Institute: University of Basrah

College of Sciences

Department of Mathematics

Email: mohna_l@yahoo.com

mohammed.ibrahim@uobasrah.edu.iq

Date: October 8, 2022

Mohammed Alabbood

MOHAMMED ALI IBRAHIM

Half of knowledge is to say "I do not know"

Contents

Chapter 1 Background

1.1 Rings

A **rng** is a set R endowed with two binary operations, usually denoted $+$ and $\cdot$, such that

- $(R, +)$ is an abelian group,
- $(R, \cdot)$ is a semigroup,
- $\cdot$ distributes over $+$.

A rng R is said to be a **ring with unity** (or sometimes a **unital ring**) if there exists an element in R, denoted by 1, which has the property that $a \cdot 1 = 1 \cdot a = a$ for all a in R (multiplicative identity=unity of R). A ring R in which $a \cdot b = b \cdot a$ for all a, b in R, is called a **commutative ring**.

Remark: The **zero ring** is a ring in which $1 = 0$. From now on, except in certain specific examples, if the term ring is used, it will mean a commutative non zero ring. That is to say, unless stated otherwise, all our rings will be unital rings.

Warmup: Let R be a ring, with additive and multiplicative identities 0 and 1, respectively. Then for all a, b in R: (1) $0a = a0 = 0$; (2) $(-a)b = a(-b) = -(ab)$; (3) $(-a)(-b) = ab$; (4) $(na)b = a(nb) = n(ab)$ for any n in $\mathbb{Z}$. Note that n is not to be thought of as an element of R: the notation na just means $a + \ldots + a$, where there are n copies of a in the sum.

Example: $\mathbb{Z}$: the integers with usual addition and multiplication, form a commutative ring. Note that we cannot always divide, since $1/2$ is no longer an integer. Similarly, the familiar number systems $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are all rings.

$\mathbb{Z}[x]$: this is the set of polynomials whose coefficients are integers.

$\mathbb{Z}[x, y, z]$: polynomials in three variables with integer coefficients.

$\mathbb{Z}/n\mathbb{Z}$: The integers $\mod n$. These are equivalence classes of the integers under

the equivalence relation "congruence $\mod n$". If we just think about addition (and subtraction), this is exactly the cyclic group of order n.

$C[0,1]$: This is the set of all continuous real-valued functions on the interval $[0,1]$ forms a ring under usual addition and multiplication of functions.

$M_n(R)$ (non-commutative): the set of $n \times n$ matrices with entries in a commutative ring R. These form a ring, since we can add, subtract, and multiply square matrices. This is the first example we've seen where the order of multiplication matters: AB is not always equal to BA (usually it's not).

1.1.1 Special elements in a ring

Let a be an element of a ring R . We say that a is:

- a **unit** if a has a multiplicative inverse, i.e., if there exists an element b in R such that $ab = ba = 1$; in this case, a is also said to be **invertible**, and b the **inverse** of a (and vice versa). Note also that b is a unit as well - units come in pairs. Of course, it's possible that $b = a$, i.e., an element may be its own inverse. The set of units in R is denoted $R^\times$- the **group of units** of R;
- a **zero-divisor** if there is a nonzero element b in R such that $ab = ba = 0$. The set of all non zero-divisors in R is denoted by $\mathsf{NZD}(R)$, and the set of zero-divisors of R is denoted by $\mathsf{ZD}(R)$;
- **nilpotent** if $a^k = 0$ for some $k \in \mathbb{Z}^+$. The set of all nilpotent elements of R is denoted by $\mathsf{Nil}(R)$;
- **idempotent** if $a^2 = a$.

Example: In $\mathbb{Z}$, the units are ∓ 1, there are no non zero-divisors and hence $\mathsf{NZD}(\mathbb{Z}) = \mathbb{Z}\backslash\{0\}$, no nilpotent elements except 0 and hence $\mathsf{Nil}(\mathbb{Z}) = \{0\}$, and only 1 is idempotent.

In $\mathbb{Q}[x]$, the units are the nonzero constant polynomials, there are no zero-divisors except the zero polynomial, and no nontrivial idempotent or nilpotent elements.

In $\mathbb{Z}/n\mathbb{Z}$, the units are those classes $\bar{m}$ for which $\gcd(m,n) = 1$. The zero-divisors are those for which $\gcd(m,n) \neq 1$ and 0. Note that $\mathbb{Z}/n\mathbb{Z} = (\mathbb{Z}/n\mathbb{Z})^\times \sqcup \mathsf{ZD}(\mathbb{Z}/n\mathbb{Z})$.

In $M_n(R)$, the units are just the invertible matrices, which is just the multiplicative

group $GL_n(R)$. There are plenty of zero-divisors: any strictly upper-triangular matrix multiplied by a matrix whose all rows zeros except the first row is zero. Also, any strictly lower-triangular matrix multiplied by a matrix whose all rows zeros except the last row is zero, so there are already lots of them. Nilpotents must have 0 as their only eigenvalue. Idempotents must be diagonalizable and have 0 or 1 as their only eigenvalue. Note that $A \in M_n(R)$ is nilpotent iff the characteristic polynomial for A is $\det(\lambda I - A) = \lambda^n$.

Fields: A nonzero ring in which every nonzero element is a unit is called a **field**.

Fields include many familiar number systems, such as $\mathbb{Q}, \mathbb{R}, \mathbb{C}$; $\mathbb{Z}$, on the other hand, is not a field.

1.1.2 Subrings

If R is a ring, and S is a subset of R. We will say that S is a **subring** of R if S is a subgroup of R under $+$, and S is closed under multiplication.

IMPORTANT: For the remainder of these lectures, all rings will be assumed commutative with unity, without further mention, unless explicitly stated otherwise.

We will discuss how to easily get new rings out of other rings by finding rings inside others (subrings) or by combining rings together.

Example: $\mathbb{Z}$ is a subring of $\mathbb{Z}[x]$, which is in turn a subring of $\mathbb{Z}[x, y, z]$, etc.

$\mathbb{Z}$ is a subring of $\mathbb{Q}$, which is a subring of $\mathbb{R}$, etc.

In general, there is a construction called **adjoining an element** defined as follows: start with a ring R, and add a new element x. This x could be a "formal variable", or it could be a known element of some other ring containing R. We build a **ring of polynomial** $R[x]$ (read as R adjoin x). An element in $R[x]$ has the form $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$, where the $a_i \in R$. The construction of $R[x]$ realizes R as a subring of a larger ring.

The **Gaussian integers** are defined as the subring of $\mathbb{C}$ given by adjoining i to the integers, namely $Z[i]$. They can be pictured as a square lattice in the complex plane. They contain $\mathbb{Z}$ as a proper subring.

Rings such as $\mathbb{Q}[\sqrt{2}]$, where we adjoin an irrational square root to the rational

numbers, are of great importance in number theory. They are called **quadratic number fields**. Since $(\sqrt{2})^2 \in \mathbb{Q}$, we don't need any higher powers of the new element $\sqrt{2}$, so actually $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. In other words, if we think of this as some set of polynomial ring, where the "variable" is $\sqrt{2}$, then actually the only polynomials we need are linear.

Products of Rings: Let R and S be two rings. Their product, sometimes called the **direct product**, denoted $R \times S$, is the ring

$$R \times S = \{(r, s) : r \in R, s \in S\}.$$

So as a set, $R \times S$ is just the Cartesian product. It's made into a ring by defining addition and multiplication componentwise:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2); \quad (r_1, s_1) \cdot (r_2, s_2) = (r_1 r_2, s_1 s_2).$$

The zero element (additive identity) of this ring is just $(0, 0)$- note that the First zero lives in R, but the second lives in S, so it's bad notation. The multiplicative identity is $(1, 1)$. Inside $R \times S$, there is "a copy" of R, namely the set $R \times \{0\} = \{(r, 0) : r \in R\}$. Products of rings always have lots of zero-divisors. For example, in $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$, if a, b are nonzero integers, then $(a, 0)$ and $(0, b)$ are nonzero elements whose product is zero, so they are zero-divisors.

Products of rings also have nontrivial idempotents, which is a comparatively rare phenomenon. For instance, $\mathbb{Z}$ has no nontrivial idempotents, whereas $\mathbb{Z} \times \mathbb{Z}$ has the idempotents $(1, 0)$ and $(0, 1)$.

1.1.3 Ring Homomorphisms

Just as with groups, when we study rings, we are only concerned with maps that "preserve the structure" of a ring, and these are called ring homomorphisms. Maybe you can guess what the definition should be, by analogy with the case of groups.

Ring homomorphisms: Let R and S be rings, and $\phi : R \to S$ be a map. We say ϕ is a **ring homomorphism** if, for all a, b in R,

- $\phi(a + b) = \phi(a) + \phi(b)$,
- $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$,
- $\phi(1) = 1$.

Note that in last condition, the first 1 is in R, while the second 1 is in S. Notice that we explicitly require that ϕ sends 1 to 1. What about the additive identity 0? Why don't we have to require that $\phi(0) = 0$? This is because, R and S are groups under addition and ϕ is a group homomorphism, it follows automatically. But since neither R or S are groups under multiplication, we have to add in this condition separately.

Let R and S be two rings. The set of all homomorphisms from R to S is denoted $\mathsf{Hom}(R, S)$.

A homomorphism is **injective** or **surjective** if it so as a map of sets (i.e., the usual definitions apply).

The map $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(n) = n + 1$ is not a ring homomorphism. It fails conditions $1, 2$, and 3. In fact, there is only one ring homomorphism from $\mathbb{Z}$ to $\mathbb{Z}$, the identity map, which sends each integer to itself. This is one of the reasons why $\mathbb{Z}$ is a very important ring.

The map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ which sends an integer m to its congruence class $\bar{m} \mod n$ is a ring homomorphism.

$\mathsf{Ev}_a : \mathbb{Z}[x] \to \mathbb{Z}$ given by $\mathsf{Ev}_a(p(x)) = p(a)$ is a ring homomorphism, called the **evaluation map** at a. It means simply "plug in a". This type of homomorphism is ubiquitous, since polynomials can be viewed as polynomial maps, and for maps we just "plug in" an element. One can define the same sort of map with $\mathbb{Z}$ replaced by an arbitrary ring R. In fact, if R is any ring, then there are lots of homomorphisms from $\mathbb{Z}[x]$ to R. All we have to do is pick an element r in R, and send x to r.

The map $\mathbb{Z} \to \mathbb{Z}$ sending n to n^k is not a ring homomorphism unless $k = 1$. For example, if $k = 2$, then since $2 = 1^2 + 1^2 \neq (1 + 1)^2 = 4$, it is not additive.

If p is a prime, and R is a ring in which $p = 1 + 1 + \ldots + 1 = 0$, then the map $R \to R$ which sends r to r^p is a ring homomorphism. In other words, when we work $\mod p$, the pth power map is a ring homomorphism. Contrast this with the previous example.

Just as for groups, bijective homomorphisms are called isomorphisms, and they tell us when two rings "have the same structure".

Ring isomorphisms: An **isomorphism** from a ring R to another ring S is a bijective

homomorphism. If an isomorphism between R and S exists, then we say R and S are **isomorphic** and we write $R \cong S$.

There is an alternative way to characterize isomorphisms, using inverse maps.

Proposition: Let $f : R \to S$ be a homomorphism. Then f is an isomorphism if and only if there exists a homomorphism $g : S \to R$ such that $g \circ f$ is the identity map on R and $f \circ g$ is the identity map on S.

Proof $g \circ f = I_R$ implies f is injective, and g is surjective. Similarly, $f \circ g = I_S$ implies g is injective, and f is surjective.

Example: For any ring R, the set $\mathsf{Hom}(\mathbb{Z}[x], R)$ is in bijection with R. Moreover, $\mathsf{Hom}(\mathbb{Z}[x], R) \cong R$. In fact, define a bijection from R to $\mathsf{Hom}(\mathbb{Z}[x], R)$ that send r in R to Ev_r in $\mathsf{Hom}(\mathbb{Z}[x], R)$.

Remark: The example above can be restated as follows: a homomorphism out of $\mathbb{Z}[x]$ is uniquely determined by where it sends x. An analogous statement is true for maps out of $\mathbb{Z}[x, y]$, etc.

Example: Inside the matrix ring $M_2(\mathbb{R})$, there is a subring

$$R = \left\{ \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} : n \in \mathbb{Z} \right\}.$$

Even though $M_2(\mathbb{R})$ is not a commutative ring, the subring R is commutative, and it is isomorphic to $\mathbb{Z}$.

The kernel of a homomorphism: Let $\phi : R \to S$ be a homomorphism of rings. The **kernel** of ϕ, denoted $\ker \phi$, is the subset $\{r \in R : \phi(r) = 0\}$ of R. In other words, it's the pre-image of 0 under ϕ.

The **image** of ϕ is the set $\mathsf{im}\phi = \{s \in S : s = \phi(r) \text{ for some } r \in R\}$.

The image of a homomorphism is a subring of the codomain; the kernel is a subring of the domain.

Example: The kernel of $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ sending m to $\bar{m}$ is $\{kn : k \in \mathbb{Z}\}$, in other words, the set of all multiples of n.

The kernel of $\phi : \mathbb{Z}[x] \to \mathbb{Z}[x]$ sending $p(x)$ to $p(1)$ is the set of all multiples of $x - 1$.

The kernel of the map $\mathbb{Z}[x] \to \mathbb{Q}$ which sends x to $1/2$ is the set of all multiples of $2x - 1$.

The kernel of the map $\mathbb{Z}[x] \to \mathbb{Z}_2[x]$ which sends a polynomial $p(x)$ to the congruence class $\overline{p(x)}$ (in other words, "reduce the coefficients $\mod 2$") is the set of all polynomials with even coefficients.

Remark: Just as for groups, the kernel and image detect injectivity and surjectivity: to be injective means to have a trivial kernel, so maps with a large kernel can be thought of as "very un-injective".

Warmup: Let $f : R \to S$ be a homomorphism of rings. Then f is injective if and only if $\ker f = \{0_R\}$; f is surjective if and only if $\mathrm{im} f = S$.

1.1.4 Ideals

An ideals is in some ways like a normal subgroup, and in some ways like a vector subspace in linear algebra.

Ideals: Let R be a commutative ring. A subset I of R is called an **ideal** if it satisfies the following conditions: (1) I is an additive subgroup of R under $+$ (additive subgroup); (2) For any i in I and any element r of R, $r \cdot i$ is in I (closed under scaling).

Remark: We call the second condition "closed under scaling" to distinguish it from "closed under multiplication". We borrow the term from linear algebra. Notice that in the definition we required the ring R to be commutative. This isn't a big deal for us since most of our rings are commutative anyway. In a noncommutative ring there are notions of left ideals, right ideals, and two-sided ideals, depending on wether I is closed under scaling on the left, the right, or both. As we can imagine, this complicates things quite a bit, and is one of the reasons why noncommutative rings are much harder to study.

Proposition: If $f : R \to S$ is a homomorphism, $\ker f$ is an ideal of R.

Proof Exercise.

Example: Every ring has at least one ideal: the subset consisting of only 0. It's an additive subgroup, and closed under scaling because anything times zero is zero. We denote it by either (0) or just simply 0.

In $\mathbb{Z}$, for any n, the set $\langle n \rangle$ of all multiples of n is an ideal.

Similarly, in a polynomial ring $\mathbb{Z}[x]$ (or $\mathbb{R}[x]$, etc), for any polynomial $p(x)$, the set $\langle p(x) \rangle$ of all multiples of $p(x)$ is an ideal.

In a polynomial ring $\mathbb{Z}[x]$ (or $\mathbb{R}[x]$, etc), for any element a of $\mathbb{Z}$ (or $\mathbb{R}$, etc) the set of polynomials which go to zero when you plug in a for x forms an ideal. You might recognize this as the kernel of the map $p(x) \mapsto p(a)$.

In any ring R, the entire ring R is itself ideal, called the "unit ideal". The reason for this name is: if an ideal I contains 1, then it is equal to the entire ring, because if 1 is in I, then for any r, $r = r \cdot 1$ is also in I by closure under scaling. This is the largest ideal in R.

What are all possible ideals in $R = \mathbb{Z}/6\mathbb{Z}$? This is a classic exam-style question. Let's work it out - let I be a "mystery" ideal. I will just write elements as integers, but they're all to be taken $\mod 6$. First of all, if 1 is in I, then $I = R$, so from now on let's assume that 1 is not in I. We know 0 must be in I, and that if nothing else is, then I is just the zero ideal. So now let's assume that there is at least one other element a in I, which is nonzero, and not equal to 1. If $a = 5$, then since $5 \cdot 5 = 25 = 1$, I would contain 1, and hence be the unit ideal again. So let's assume $a \neq 5$, either. If $a = 3$, then the only multiples of $a \mod 6$ are 3 and 0, so in this case $I = \{0, 3\}$. If $a = 2$, then all the multiples of $2 \mod 6$ are $0, 2, 4$, we get $I = \{0, 2, 4\}$. Similarly if $a = 4$. What if I contains 2 and 3? Then by closure under addition it contains 5 as well, and then I would be the unit ideal as above. Similarly, if I contains one even and one odd number $\mod 6$, then we just get the unit ideal. So the possible ideals in $\mathbb{Z}/6\mathbb{Z}$ are $0, R, \langle \bar{2} \rangle, \langle \bar{3} \rangle$. Note we have used the notation $\langle \cdots \rangle$ as in the examples above to denote the set of multiples of a given element. These types of ideals come up so often that they have a special name:

Ideal generated by a set: Let X be any subset of a ring R. The **ideal generated by** X is the smallest ideal containing all elements of X, and is denoted by $\langle X \rangle$. It can also be described as the set of all "R-linear combinations" of elements of X with coefficients in R. Elements of X are called generators of the ideal. If X is a finite set, say $X = \{x_1, \ldots, x_k\}$, we will write this ideal "**finitely generated ideal**" as $\langle x_1, \ldots, x_k \rangle$. In the case when X is a singleton, $X = \{x\}$, the ideal $\langle x \rangle$ is called **principal**.

Remark: Note that there may be many different choices of generators for a given

ideal. For example, $\langle n \rangle = \langle -n \rangle$ inside $\mathbb{Z}$; $\langle x \rangle = \langle 5x \rangle$ inside $\mathbb{R}[x]$ (but not when considered as ideals in $\mathbb{Z}[x]$- do you see why not?). Note that $\langle 2, x \rangle = \langle 4, x - 2 \rangle$ inside $\mathbb{Q}[x]$. In fact, even the number of generators can be ambiguous: the ideals $\langle 2 \rangle$ and $\langle 4, 6 \rangle$ are equal in $\mathbb{Z}$.

Principal ideals are the nicest possible ideals you can have, and there are lots of rings in which every ideal is principal, including $\mathbb{Z}$ and $\mathbb{Q}[x]$. These nice rings are called principal ideal domains, and we will study them more later.

Warmup: Let I be an ideal in R. I contains a unit if and only if $I = R$.

Operations on Ideals: The following proposition gives ways to produce new ideals, both larger and smaller, from given ideals.

Proposition: Let $\{I_a\}_{a \in A}$ be an arbitrary collection of ideals in a ring R, indexed by a set A. Then

- $\bigcap_{a \in A} I_a$ is an ideal in R.
- $I_a + I_b = \{x + y : x \in I_a, y \in I_b\}$ is an ideal, called the sum of I_a and I_b. It is the smallest ideal in R which contains both I_a and I_b.

Proof Exercise.

Example: Let $I = \langle x^2, y \rangle$, $J = \langle x, y^2 \rangle$ in $\mathbb{C}[x, y]$. Then $I \cap J = \langle x^2, xy, y^2 \rangle$, while $I + J = \langle x, y \rangle$.

Let $m, n \in \mathbb{Z}$ be coprime. Then $\langle m \rangle \cap \langle n \rangle = \langle mn \rangle$, while $\langle m \rangle + \langle n \rangle = \langle 1 \rangle = \mathbb{Z}$. This second is another way of stating the fact that if $\gcd(m, n) = 1$, then there are integers a, b such that $am + bn = 1$.

1.1.5 Quotient Rings

We know that if we have a set S, and we choose an equivalence relation on it, we can partition our set into equivalence classes, which are disjoint and whose union is the entire set. Elements are in the same equivalence class if and only if they are equivalent under the relation we chose at the beginning. We also know that conversely, any way we partition our set gives rise to an equivalence relation- we simply define two elements to be equivalent whenever they live in the same piece of the partition.

The idea of a coset in ring theory is basically the same as in group theory, except with ideals replacing subgroups. Let's go through it: let R be a ring, and I an ideal in R. First we define our equivalence relation: elements a, b of R are equivalent, written $a \sim b$, when $a - b$ is in I. Then by the general theory discussed in the previous paragraph, this partitions our ring into disjoint subsets, called cosets. One of the cosets is just I itself: this is the equivalence class of 0, since $a \sim 0$ exactly when $a = a - 0 \in I$. The other cosets look similar to I, they've just been "translated" by elements of R. We will write R/I for the set of cosets of I.

For a familiar example, take R to be $\mathbb{Z}$, and I to be the ideal $\langle 3 \rangle$. Then the cosets are $\langle 3 \rangle$ itself, and the two other subsets $\{\ldots, -2, 1, 4, \ldots\}$ and $\{\ldots, -1, 2, 5, \ldots\}$. They look the same (integers spaced 3 apart), but just "shifted".

Quotient Rings: Now that we've defined the cosets, we want a way to turn the set of cosets R/I into a ring itself, and this is where the fact that I is an ideal comes into play. To fix notation, R is our ring, I our ideal in R, and if r is an element of R we write $\bar{r}$ for the coset containing r- another way of writing it is $r + I = \{r + i : i \in I\}$, namely the elements of I all shifted by r. We sometimes call r a **representative** of r. The annoying part is that there may be many choices of representative for the same coset - this is where that stuff about things being "well-defined" comes in to play. We can add cosets in the same way as for groups: $\overline{r_1} + \overline{r_2} = \overline{r_1 + r_2}$. One has to fuss about to prove that this addition rule is well-defined, but we'll skip that since we did it for groups and we're about to do it again for the multiplication of cosets. We multiply cosets in the obvious way: $\overline{r_1} \cdot \overline{r_2} = \overline{r_1 \cdot r_2}$. Now let's check this is well-defined. Suppose r_1 and s_1 are both representatives of the same coset (so $\overline{r_1} = \overline{s_1}$), and that r_2 and s_2 also represent the same coset. We need to check that whether we multiply the cosets using the r's or the s's we'll get the same answer. That's what it means to check that the multiplication is well-defined. In other words, we must show that $\overline{r_1} \cdot \overline{r_2} = \overline{s_1} \cdot \overline{s_2}$. Since r_1 and s_1 represent the same coset, they are equivalent (since cosets are equivalence classes), which means there is an element i_1 of I such that $r_1 = s_1 + i_1$. Similarly there is an i_2 such that $r_2 = s_2 + i_2$. This means that

$$\begin{aligned}\overline{r_1} \cdot \overline{r_2} = \overline{r_1 \cdot r_2} &= \overline{(s_1 + i_1)(s_2 + i_2)} \\ &= \overline{s_1 s_2 + s_1 i_2 + s_2 i_1 + i_1 i_2} = \overline{s_1 s_2} = \overline{s_1} \cdot \overline{s_2}.\end{aligned}$$

We should be able to go through and justify why each equality is true. The trickiest one

is the fourth: the cosets $\overline{s_1s_2 + s_1i_2 + s_2i_1 + i_1i_2}$ and $\overline{s_1s_2}$ are the same because the two representatives are equivalent: $(s_1s_2 + s_1i_2 + s_2i_1 + i_1i_2) - (s_1s_2) = s_1i_2 + s_2i_1 + i_1i_2$, which is in I. You can see here why we need property 2 of the definition of an ideal. We want $s_1i_2 + s_2i_1 + i_1i_2$ to be in I, and it wouldn't be if I were only closed under multiplication, since s_1 and s_2 do not necessarily live in I.

There's a lot more left to show that this addition and multiplication make R/I into a (commutative) ring (with unity): we have to check all the axioms for a (commutative) ring (with unity)! we won't type that all out in great detail. First of all, R/I has a zero element, which is just the coset I (usually represented by the element 0 in R). Often we will write 0 instead of the coset notation $\bar{0}$. Secondly, as you might guess, R/I has a multiplicative identity, which is just the coset $\bar{1}$. Again we may often write simply 1 instead of the coset notation $\bar{1}$. We don't really need to check the axioms stating that R/I is an additive abelian group, since we've already done that when we discussed quotient groups. The other axioms basically follow from the corresponding property for R. For instance, here's a proof that left-distributivity holds. Let a, b, c be elements of R. Then

$$\bar{a} \cdot (\bar{b} + \bar{c}) = \overline{a \cdot (b + c)} = \overline{a \cdot b + a \cdot c} = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}.$$

Example: Take $R = \mathbb{Z}$ and $I = \langle n \rangle$. Then $R/I = \mathbb{Z}/n\mathbb{Z}$, and this is just the usual integers $\mod n$, where we do all the addition and multiplication $\mod n$.

Take $R = \mathbb{C}[x]$, and $I = \langle x - 2 \rangle$. We said before that the coset I acts as the zero element in R/I, so $\overline{x - 2} = 0$. This is the same, using the addition rule for cosets, as saying that $\bar{x} = \bar{2}$. So how does R/I look? Well, it's just like the polynomial ring, except we've replaced x with 2 and put bars over everything. Since 2 is already in $\mathbb{C}$, we haven't really added anything, so in fact this quotient ring is just like $\mathbb{C}$.

Take $R = \mathbb{R}[x], I = \langle x^2 + 1 \rangle$. In the quotient ring $\mathbb{R}[x]/\langle x^2 + 1 \rangle$, we have cosets of polynomials, but with the rule that x $\overline{x^2 + 1} = \bar{0}$, which we rewrite as $\bar{x}^2 = -\bar{1}$. So we think of elements of R/I here as polynomials, but with the extra rule that $\bar{x}^2 = -1$. This is something we've seen before: it's basically the same as $\mathbb{C}$, where we take $\mathbb{R}$ and adjoin a square root of -1, which in the current setting is being denoted by $\bar{x}$.

Let's work backwards a bit. Say we want to work with a number system that's like the rational numbers, but also for some reason includes the element $\sqrt{2}$. We can build this number system, namely $\mathbb{Q}[\sqrt{2}]$, using quotient rings. Start with $\mathbb{Q}$. We'll need to

adjoin a variable (call it x), and then set this variable equal to $\sqrt{2}$. We cannot just quotient out by $(x-\sqrt{2})$ because that's not a polynomial with rational coefficients. So the correct quotient ring seems like it should be $\mathbb{Q}[x]/\langle x^2-2\rangle$. So the ring $\mathbb{Q}[x]/\langle x^2-2\rangle$ is like the rationals, but with an extra symbol $\bar{x}$, which we know should behave like $\sqrt{2}$, namely $\bar{x}^2 = \bar{2}$. We can say that $\mathbb{Q}[x]/\langle x^2-2\rangle \cong \mathbb{Q}[\sqrt{2}]$, where the latter is to be thought of as a subring of $\mathbb{R}$ (or $\mathbb{C}$).

Let $R = \mathbb{R}[x]$ and I be the ideal generated by $x^3 - 1$. Now we're going to stop writing the bars on top of everything, for simplicity. So we think of elements of this ring as polynomials in x, but subject to the relation $x^3 = 1$. What is $(x^4 - x^2)$ times (x^2+x+1) in this ring? It doesn't have degree 6, like we'd expect in a normal polynomial ring. First we can simplify the first one to $x - x^2$ using the relation, and then multiply them out to give

$$(x - x^2)(x^2 + x + 1) = x^3 + x^2 + x - x^4 - x^3 - x^2 = x - x^4,$$

and since $x^3 = 1$, $x^4 = x$, so this is just zero! So the first thing we notice is that this ring has zero divisors - we just found two of them - $x^4 - x^2$ and $x^2 + x + 1$. There is a more enlightening way to see that their product is zero, however, by diligently factoring everything first:

$$(x^4 - x^2)(x^2 + x + 1) = x^2(x + 1)(x - 1)(x^2 + x + 1) = x^2(x + 1)(x^3 - 1).$$

This shows that their product is a multiple of x^3-1, hence lies in I. So $(x^4-x^2)(x^2+x+1)$ and $x^3 - 1$ are equivalent, hence the coset $[(x^4 - x^2)(x^2 + x + 1)]$ is the same as the coset $[x^3 - 1]$, which is just I, and we know that this functions as the zero element in the quotient ring. Notice that the zero divisor phenomenon basically happened because the generator for I factored: $x^3 - 1 = (x - 1)(x^2 + x + 1)$. That means right away that the two polynomials $x - 1$ and $x^2 + x + 1$ are zero divisors. We'll come back to this when we discuss prime ideals.

Here's a cool example that shows how you can do calculus without limits. Start with the ring $\mathbb{R}[x]$, and adjoin a new element ϵ, giving the ring $\mathbb{R}[x][\epsilon] = \mathbb{R}[x, \epsilon]$. Finally, take the quotient by the ideal $\langle\epsilon^2\rangle$, this forces ϵ to satisfy the relation $\epsilon^2 = 0$. Let $R = \mathbb{R}[x, \epsilon]/\langle\epsilon^2\rangle$ be this new ring. We can compute derivatives in this ring as follows: pick a polynomial whose derivative you want to compute, say $f(x) = x^3$. Now look at

$$f(x + \epsilon) = (x + \epsilon)^3 = x^3 + 3x^2\epsilon + 3x\epsilon^2 + \epsilon^3 = x^3 + 3x^2\epsilon.$$

All the higher ϵ terms disappear because of the relation $\epsilon^2 = 0$, and the coefficient of the remaining ϵ term is just $3x^2$, the derivative! In a HW exercise you will be asked to prove that in general,

$$f(x + \epsilon) = f(x) + f'(x)\epsilon.$$

If we work instead with the relation $\epsilon^n = 0$, when we expand $f(x + \epsilon)$, you will get the first $n + 1$ terms of the Taylor series for f.

1.1.6 The Isomorphism Theorem for rings

This section contains an extremely powerful result, which we remember as saying "image = source/kernel". This is entirely analogous to the isomorphism theorem we saw for groups. Recall that the image of a map of rings $\phi : R \to S$ is the subring

$$\mathrm{im}\phi = \{s \in S : \text{there exists an } r \in R \text{ such that } \phi(r) = s\}.$$

Proposition: Let $\phi : R \to S$ be a homomorphism of rings, and let $I \subseteq R$ be its kernel. Then $\mathrm{im}\phi \cong R/I$.

Proof (Hint) As usual we have to define an isomorphism $f : R/I \to \mathrm{im}\phi$. Let $\bar{r} \in R/I$ be a coset, and define $f(\bar{r}) = \phi(r)$.

Example: First we'll use the proposition to give a proof that $\mathbb{R}[x]/\langle x^2 + 1\rangle \cong \mathbb{C}$, which we showed in the previous section. The idea is to first give a map from $\mathbb{R}[x]$ to $\mathbb{C}$, find its kernel, and apply the theorem. The map we'll use is $\phi : \mathbb{R}[x] \to \mathbb{C}$ given by $p(x) \mapsto p(i)$. Like we did before, but now x really means x , and not the coset $[x]$. It's surjective, because for any $a + bi$ in $\mathbb{C}$, we have $\phi(a + bx) = a + bi$; so $\mathrm{im}\phi = \mathbb{C}$. To find the kernel, suppose $\phi(p) = 0$. Then $p(i) = 0$, so p has i as a root; since it's a real polynomial, it must also have $-i$ as a root, too (complex roots of real polynomials always come in conjugate pairs...). This means that if we factor p over $\mathbb{C}$, it has factors $x - i$ and $x + i$, so over $\mathbb{R}$, it has a factor $x^2 + 1$. Thus p is in the ideal generated by $x^2 + 1$. Conversely, every element of the ideal $\langle x^2 + 1\rangle$ is in kernel, so this shows $\ker\phi = \langle x^2 + 1\rangle$. Applying the theorem then gives $\mathbb{R}[x]/\langle x^2 + 1\rangle \cong \mathbb{C}$.

For an easier example, consider the ring $\mathbb{R}[x]/\langle x - 1\rangle$. We know that the quotient here basically means "set x equal to 1", and since 1 is already in $\mathbb{R}$, this quotient ring should just be $\mathbb{R}$. So define $\phi : \mathbb{R}[x] \to \mathbb{R}$ by sending x to 1; that is to say, $\phi(p(x)) = p(1)$

(so ϕ is just the evaluation map Ev_1). In fact,

$$\mathbb{R} = \mathsf{im}\phi \cong \mathbb{R}[x] = \ker \phi = \mathbb{R}[x]/\langle x - 1\rangle).$$

1.1.7 Division and Factorization in $\mathbb{Z}$

First we recall mostly without proof the basic multiplicative properties of $\mathbb{Z}$.

Proposition: If a and b are two integers, with $b \neq 0$, then there exist unique integers q and r, with $0 \leq r < |b|$, such that $a = bq + r$.

We say that b **divides** a if $a = bk$ for some integer k, and this happens if and only if $r = 0$ in the proposition. Using this, one can prove that any pair of nonzero integers a, b has a $\gcd$, and that the $\gcd$ can be expressed as an integer linear combination of a and b, in particular

Proposition: If a and b are coprime, then there exist integers x and y such that $ax + by = 1$.

The definition of a prime integer is an integer greater than one which has no factors except 1 and itself. The above proposition shows that

Proposition: If p is prime and p divides ab, then $p|a$ or $p|b$.

Proof Assume that $p|ab$. We show that if $p \nmid a$, it forces $p|b$. So assume that $p \nmid a$. Then p and a are coprime (since p has no nontrivial factors), so we can find x, y with $px + ay = 1$. Multiply by b to give $pbx + aby = b$. Since p divides both terms on the left, it divides b.

Finally, the most famous result about primes is that they are "multiplicative building blocks" for $\mathbb{Z}$.

Proposition: (Fundamental Theorem of Arithmetic). If n is any integer, then n can be written as

$$n = cp_1 \dots p_r,$$

where the p_i are primes and $c = \mp 1$. This expression is unique except for the order of the prime factors.

1.1.8 Division and Factorization of Polynomials

To keep the theory of polynomials manageable, we will be considering mostly polynomials whose coefficients live in $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$ (as opposed to $\mathbb{Z}$, where there aren't enough units, or say $\mathbb{Z}/6\mathbb{Z}$, where there are zero divisors).

We will denote by k an arbitrary field, but you should keep the examples $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ in our mind. In the division algorithm for $\mathbb{Z}$, the remainder r is "small", i.e. less than $|b|$. For this we had to measure the "size" of b using absolute value (since b might be negative). Polynomials also have a measure of size, namely their degrees.

Degree of a polynomial: Let $p \in k[x]$ be a nonzero polynomial, written as $p(x) = a_n x^n + \ldots + a_1 x + a_0$, where $a_n \neq 0$. The degree of p is n, written $\deg p = n$. In other words, the degree of p is the largest exponent of x which appears with nonzero coefficient.

Remark: Note that we did not define the degree of the zero polynomial, for technical reasons. Polynomials of degree zero (and also the zero polynomial, whose degree is undefined) are called constant polynomials; degree one, linear; degree two; quadratic; then cubic, quartic, etc.

As for integers, we say f **divides** g in $k[x]$, written $f|g$, if there is an $h \in k[x]$ such that $g = fh$. Then f is said to be a **divisor** or **factor** of g. The notion of irreducibility, like primeness for integers, is a sort of minimality condition for the divides relation:

Irreducible polynomials: A polynomial $p \in k[x]$ is **irreducible** if p is non-constant and the only divisors of p which have lower degree are the constant polynomials.

The main results about divisibility and factorization for polynomials in $k[x]$ are the following:

Theorem:

1. If $f, g \in k[x]$ and $g \neq 0$, then there exist polynomials $q, r \in k[x]$ such that $f = gq + r$, with either $r = 0$ or $0 \leq \deg r < \deg g$.
2. If f and g have no nonconstant common factor then there are polynomials r, s such that $fr + gs = 1$.
3. If $p \in k[x]$ is irreducible and $p|fg$, then $p|f$ or $p|g$.

4. Every nonzero polynomial f can be written as $f = cp_1 \dots p_r$, where c is a unit (a nonzero constant polynomial) and the p_i are irreducible polynomials.

Proof Omitted. Part 1 is basically just long division of polynomials as you learned in high school. Parts 2, 3, and 4 follow from 1 using the same arguments as for integers.

Remark: In the factorization in 4, we can even omit the unit term c, since cp_1 will still be irreducible, so we could just rename cp_1 as p_1. However, we will often try to work with monic polynomials, i.e., those whose leading coefficient is 1. In this case, if we take all the p_i to be monic, then the unit factor c (which would just be the product of the leading terms of the p_i) appears out front.

Root (or zero) of a polynomial: Let $f \in k[x]$. An element $\alpha \in k$ is called a **root** (or **zero**) of f if $f(\alpha) = 0$ in k. Equivalently, α is a root of f if $f \in \ker \mathsf{Ev}_\alpha$. If K is a larger field containing k, we also say that $\alpha \in K$ is a root of f in K if $f(\alpha) = 0$ in K.

Remark: Note that it makes sense to evaluate $f(\alpha)$, even when $\alpha \in K \backslash k$, because since $k \subseteq K, k[x] \subseteq K[x]$, so we can regard f also as an element of $K[x]$ and apply the evaluation map $\mathsf{Ev} : K[x] \to K$ to f. The next proposition says that finding roots is the same as finding linear factors.

Proposition: Let $f \in k[x]$. Then f has a root in k if and only if f has a linear factor.

Proof First suppose that f has a linear factor, so we can write $f(x) = (x - c)g(x)$ for some $c \in k$, $g \in k[x]$. Then $f(c) = (c - c)g(c) = 0$, so f has the root c in k. Conversely, suppose f has a root c in k. Then $f \in \ker \mathsf{Ev}_c : k[x] \to k$. Also, the polynomial $x - c$ is in $\ker f$. Now apply the division algorithm to f and $x - c$, giving $f = (x-c)q+r$, where $r = 0$ or $\deg r < \deg(x-c) = 1$, so r must be a constant (either it's 0 or it has degree zero, meaning it's a nonzero constant). Call this constant a. Then $f(x) = (x-c)q(x)+a$. Plugging in $x = c$ gives $0 = f(c) = (c-c)q(c)+a = 0+a = a$, so $a = 0$. Thus $f = (x - c)q$, so f has a linear factor.

Now let's see how these factorizations look over various fields of interest.

Example: Over $\mathbb{C}$, every nonconstant polynomial has a root. So it has a linear factor. Proceeding inductively, this shows that every complex polynomial factors into linear factors, i.e. every nonzero $f \in \mathbb{C}[x]$ can be written as $f(x) = c(x - a_1)^{r_1} \dots (x - a_n)^{r_n}$

for some $c \neq 0$ and a_i in $\mathbb{C}$, and $r_i \in \mathbb{N}$. If some exponent $r_i > 1$, a_i is called a **multiple root**, and r_i its **multiplicity**. If $r_i = 1$, a_i is called a **simple root**. In other words, the irreducible polynomials over $\mathbb{C}$ are the linear ones.

Over $\mathbb{R}$ things are slightly more complicated. There are two types of irreducibles in $\mathbb{R}[x]$: linear ones and irreducible quadratics. We can tell whether a quadratic ax^2+bx+c is irreducible by looking at the **discriminant** $b^2 - 4ac$. If $b^2 - 4ac < 0$, it's irreducible, and vice versa. The way to see that these are the only irreducibles is by taking a real polynomial $f \in \mathbb{R}[x]$, and viewing it temporarily as an element of $\mathbb{C}[x]$ (which contains $\mathbb{R}[x]$). It factorizes completely into linear factors over $\mathbb{C}$, and it's easy to check that the non-real roots come in complex conjugate pairs $a_i, \overline{a_i}$. For each such pair we obtain a real irreducible quadratic, because

$$(x - a)(x - \bar{a}) = x^2 - (a + \bar{a})x + |a|^2,$$

and we can check that the discriminant of this thing is negative.

Over $\mathbb{Q}$ things are even worse! Not only are there linear and quadratic irreducibles, like in $\mathbb{R}$, but in fact there are irreducibles of every degree! For example, if p is prime, the polynomial $x^{p-1} + x^{p-2} + \ldots + x + 1$ is irreducible. This is a very interesting polynomial, called a **cyclotomic polynomial**, which can be thought of as $x^p - 1/x - 1$. It's roots are the pth roots of unity (except 1 itself).

Irreducibility is fussy over $\mathbb{Z}$ as well. For example, the polynomial $3x - 3$ is irreducible over $\mathbb{Q}$, because even though we can factor it as $3(x - 1)$, 3 is a unit in $\mathbb{Q}$. But over $\mathbb{Z}$, 3 is not a unit, so $3x - 3$ is reducible. Thus the issue of (ir)reducibility is complicated by the existence of fewer units.

Luckily there is a useful result called Eisenstein's Criterion that helps allows us to identify some of the irreducible polynomials over $\mathbb{Q}$:

Theorem: (Eisenstein's Criterion). Let $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$. If there is a prime p such that $p^2 \nmid a_0$, $p|a_i$ for $i = 0, \ldots, n-1$ and $p \nmid a_n$, then f is irreducible over $\mathbb{Q}$. If $\gcd(a_0, \ldots, a_n) = 1$, then f is also irreducible over $\mathbb{Z}$.

Proof First, note that: we can interpret the conditions on the coefficients in terms of reduction $\mathrm{mod} p$, as follows: letting $\bar{f}$ be the reduction of f $\mathrm{mod} p$ (or $\mathrm{mod} p^2$), i.e., the image of f under the map $\mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$ (or $\mathbb{Z}[x] \to \mathbb{Z}/p^2\mathbb{Z}[x]$), the conditions say that $\bar{f} = \overline{a_n} x^n$, with $\overline{a_n} \neq 0 \bmod p$, and $f = \overline{a_n} x^n + \overline{a_0} \bmod p^2$, with $\overline{a_n} \neq 0$ and $\overline{a_0}$ a

multiple of $p \bmod p^2$.

Now, suppose the conditions of the theorem hold, and assume for a contradiction that f is reducible in $\mathbb{Q}[x]$, so that $f = gh$ for some non-unit $g, h \in \mathbb{Q}[x]$. By a corollary of Gauss' Lemma, we find that f is reducible in $\mathbb{Z}[x]$ as well. Then denoting by f, g, h the reductions $\bmod p$ of these polynomials, we have $\bar{g}\bar{h} = \bar{f} = \overline{a_n}x^n$, which means that $\bar{g} = \bar{a}x^k$ and $\bar{h} = \bar{b}x^{n-k}$. This shows that all the other coefficients of g and h are zero $\bmod p$, so they're all divisible by p. But since their constant terms are both divisible by p, the constant term of f is divisible by p^2, which contradicts the hypothesis of the theorem.

Example: The polynomial $f(x) = 2x^3 + 6x^2 + 12x + 6$ is irreducible over $\mathbb{Q}$, since the prime 3 divides all but the leading coefficient, but 3^2 does not divide the constant term. Yet it is not irreducible over $\mathbb{Z}$ because we can factorize it as $2(x^3 + 3x^2 + 4x + 3)$, and this is a nontrivial factorization since 2 is not a unit in $\mathbb{Z}$.

The theorem does not apply to the polynomial $x^2 + 5x + 6$, since there is no prime which divides the lowest two coefficients. However, this polynomial is nevertheless reducible, since it factorizes as $(x + 2)(x + 3)$.

The theorem does not apply either to the polynomial $2x^2 + x + 3$, but this one happens to be irreducible, since its discriminant is $1^2 - 4 \cdot 2 \cdot 3 = -11$. This means it has two complex roots, so cannot have any integer roots. These two examples show that if we cannot find a prime p as in the statement, no conclusion whatsoever can be drawn about the irreducibility of the polynomial.

Here is a famous application. We prove that the cyclotomic polynomial $\Phi_p(x) = x^{p-1} + \ldots + x + 1$ (where p is some prime) mentioned above is irreducible in $\mathbb{Z}[x]$. First off, a trick: $\Phi_p(x)$ is irreducible if and only if $\Phi_p(x + 1)$ is (reason: $f(x) \mapsto f(x + 1)$ is an automorphism of rings). But since $\Phi_p(x) = \frac{x^p - 1}{x - 1}$, so replacing x by $x + 1$ we have

$$\begin{aligned}\Phi_p(x+1) &= \frac{1}{x}((x+1)^p - 1) \\ &= \frac{1}{x}\left(x^p + px^{p-1} + \binom{p}{2}x^{p-2} + \ldots + px\right) \\ &= x^{p-1} + px^{p-2} + \ldots + p.\end{aligned}$$

Thus Eisenstein's criterion applies and shows the irreducibility of $\Phi_p(x + 1)$, hence of $\Phi_p(x)$.

1.1.9 Special Classes of Rings

In this subsection, we define various classes of rings, and investigate the relationships between them.

Fields: A **field** is a nonzero ring in which every nonzero element is a unit. As before, we use the letter k throughout to denote an arbitrary field.

For example, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields, while $\mathbb{Z}$ is not. We proved previously that $\mathbb{Q}[\sqrt{2}]$ is a field. $\mathbb{Z}/5\mathbb{Z}$ is a field, while $\mathbb{Z}/6\mathbb{Z}$ is not. In general, $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime (you should prove this as an exercise - it follows from an analysis of the units and zero divisors in $\mathbb{Z}/n\mathbb{Z}$).

Proposition: Let R be a nonzero ring. R is a field if and only if it has exactly two ideals (which must be the zero and unit ideals).

Integral domains: A nonzero ring is called an **integral domain** (or usually simply a **domain**) if it contains no zero divisors except 0.

Example: (1) $\mathbb{Z}$ is a domain, (2) $\mathbb{Z}/n\mathbb{Z}$ is not a domain when n is composite. It is a domain when n is prime, (3) $\mathbb{Q}[x]/\langle x^2 - 1\rangle$ is not a domain, but $\mathbb{Q}[x]/\langle x^2 + 1\rangle$ is.

Principal ideal domains: An integral domain is called a **principal ideal domain** (PID for short) if every ideal in it is principal (can be generated by a single element).

Example: (1) $\mathbb{Z}$ is a principal ideal domain.
Question: what about the ideal $\langle 2, 5\rangle$ generated by 2 and 5? It has two generators, so it doesn't seem like it's a principal ideal ... Answer: since $5 - 2 - 2 = 1$ is also in this ideal, the ideal is actually the unit ideal, generated by 1, hence principal. Some ideals may not seem principal, even though they actually are.
(2) $k[x]$ is a principal ideal domain.
(3) $\mathbb{Z}[x]$ is not a principal ideal domain: the ideal $\langle 2, x\rangle$ cannot be generated by one element.
(4) $\mathbb{C}[x, y]$ is not a principal ideal domain: the ideal $\langle x, y\rangle$ cannot be generated by one element.

Euclidean Domains: An integral domain R is called a **Euclidean domain** if there is a **norm** on R, which is a function η from $R\backslash\{0\}$ to $\mathbb{N}$, which satisfies

- For any f, g in R, with g nonzero, there exist q, r in R such that $f = qg + r$, and either $r = 0$ or $\eta(r) < \eta(g)$.
- For any nonzero f, g in R, $\eta(f) \leq \eta(fg)$.

Remark: The definition says, in simple terms, that any element f can be divided by a nonzero element g, giving a remainder r that is smaller than the thing you divided by (g). The second property says that when you multiply elements, the norms get bigger (or stay the same).

Example (1) $\mathbb{Z}$ is a Euclidean domain. The norm function is just the absolute value. The fact that it satisfies the two properties is clear.
(2) $\mathbb{Q}[x]$ is a Euclidean domain. The norm function is the degree: the highest power of x appearing in the polynomial. Just as for integers, we can do long division with polynomials, and the remainder always has degree strictly less than the thing we divided by. So the first property holds. The second Property holds, and in fact $\eta(f) = \eta(g)$ if and only if they differ by a unit (recall that the units in the this ring are just the nonzero constant polynomials).
(3) The Gaussian integers $\mathbb{Z}[i]$ are a Euclidean domain with norm function given by $\eta(a + bi) = a^2 + b^2$.
(4) It can be quite hard to decide whether a given ring is a Euclidean domain or not. For how we can we prove that there does not exist a norm function? Maybe there is one, but we weren't smart enough to find it! Anyways, $\mathbb{Z}[x]$ is not a Euclidean domain. The easiest way to see this will come soon, when we prove that every Euclidean domain is a PID. Since we know that $\mathbb{Z}[x]$ isn't a PID, it cannot be a Euclidean domain, either.

Irreducible elements: A nonzero element r of a ring R is called **irreducible** if it is not a unit and the only way to factor $r = ab$ is by taking either a or b to be a unit.

Thus an irreducible element is one which is "unfactorable", except for "trivial" factorizations obtained by pulling out units. For example, prime numbers in $\mathbb{Z}$, or linear polynomials in $\mathbb{C}[x]$. Of course, in $\mathbb{R}[x]$, there are irreducible quadratics, too, such as $x^2 + 1$.

Unique factorization domains: An integral domain R is called a **unique factorization domain** (or UFD, for short) if every nonzero element that is not a unit can be written as a product of finitely many irreducible elements, and this factorization is

unique, meaning that given any two factorizations $r = a_1 \dots a_k = b_1 \dots b_m$, k and m must be the same, and after possibly reordering the factors, each a_i is a unit times b_i.

Example: (1) $\mathbb{Z}$ is a UFD - this is the statement of the fundamental theorem of arithmetic.
(2) $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x]$, and $\mathbb{C}[x]$ are all UFDs.
(3) $\mathbb{Z}/6\mathbb{Z}$ is not a UFD, because for example there are two ways to factor 3: $3 = 3 \cdot 3$ and $3 = 3 \cdot 5$. But there's a simpler reason: $\mathbb{Z}/6\mathbb{Z}$ is not even a domain! 3 is a zero divisor: if you multiply it up by 2, you get 0, so there should be many ways to factor it, by adding copies of 2 to the second factor. This is one reason why we restrict our attention to domains when talking about factorization.
(4) The most famous example of a ring that is a domain but is not a UFD is $\mathbb{Z}[\sqrt{-5}]$, which is a subring of $\mathbb{C}$. In this ring there are two ways to factor 6: $6 = 2 \cdot 3$ and $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. One has to check that $2, 3$ and $1 \mp \sqrt{-5}$ are all irreducible and do not differ by units to make sure that these really count as distinct factorizations.

We know establish some containments between these various types of rings. The results are summarized in the following theorem.

Theorem: {fields} $\subseteq$ {Euclidean domains} $\subseteq$ {PIDs} $\subseteq$ {UFDs} $\subseteq$ {IDs}

1.1.10 Prime and Maximal Ideals

In this subsection we discuss two very important types of ideals, and learn how to use them to check whether certain quotients are fields or integral domains.

Prime numbers and prime ideals in $\mathbb{Z}$: The crucial connection between (principal) ideals and elements is this: divides corresponds to contains. This means: if $f|g$ in a ring (meaning there is an h such that $g = fh$), then $g \in \langle f \rangle$. If f divides g, then g is in the ideal generated by f.

What does this mean in the simple case of the ring $\mathbb{Z}$? Prime numbers are ones that have no proper divisors. Another property, often taken as the definition, is that if a prime p divides a product, then it divides one of the factors: if $p|ab$, then $p|a$ or $p|b$. This is the property we want to generalize to ideals. So let's translate the statement. In fact, $p|ab$ means $ab \in \langle p \rangle$, and similarly $p|a$ means $a \in \langle p \rangle$, etc. So in terms of ideals, p is a prime number means that if ab is in $\langle p \rangle$, then a or b (or both) must be in $\langle p \rangle$. So for an ideal

in $\mathbb{Z}$ generated by a prime number, we have the following slogan: **if a product is in it, one of the factors must be**, also. This is basically the definition of a prime ideal, and it makes sense in any ring.

Prime Ideals: Let $\mathfrak{p}$ be a proper ideal in a ring R. We say $\mathfrak{p}$ is a **prime ideal** if whenever ab is in $\mathfrak{p}$, either a or b (or both) is in $\mathfrak{p}$. The set of all prime ideals of R is denoted by $\mathsf{Spec}(R)$.

Example: In $\mathbb{Z}$, an ideal $\langle n \rangle$ is prime if and only if the integer $|n|$ is prime (we put the absolute value since primes are required to be positive, but the generator may not be), or $n = 0$.

More generally, in any PID, a nonzero ideal is prime if and only if it is generated by an irreducible element.

In the ring $\mathbb{Z}$, the zero ideal is prime, but in the ring $\mathbb{Z}/6\mathbb{Z}$, the zero ideal is not prime, since $2 \cdot 3 \in \langle 0 \rangle$ but $2 \notin \langle 0 \rangle$ and $3 \notin \langle 0 \rangle$.

Maximal Ideals: An ideal $\mathfrak{m}$ in a ring R is called maximal if it is not the unit ideal and there are no other ideals I such that $\mathfrak{m} \subsetneq I \subsetneq R$. The set of all maximal ideals of R is denoted by $\mathsf{MaxSpec}(R)$.

Example: (1) In $\mathbb{Z}$ and $\mathbb{R}[x]$, every nonzero prime ideal is maximal.
(2) In $\mathbb{R}[x, y]$, $\langle x, y \rangle$ is maximal, $\langle x \rangle$ is prime but not maximal, and $\langle x^2 \rangle$ is neither prime nor maximal.
(3) In $\mathbb{C}[x, y]$, any ideal of the form $\langle x - a, y - b \rangle$ (where $a, b \in \mathbb{C}$) is maximal.
(4) In $\mathbb{Z}[x]$, $\langle 2 \rangle$ is prime but not maximal. The ideal $\langle 2, x \rangle$ is maximal. The ideal $\langle 4, x \rangle$ is neither prime nor maximal.

Now we prove a few useful things about these ideals. Before proving the next very useful proposition, we need a basic result about ideals in quotient rings. Recall that the **canonical homomorphism** $\pi : R \to R/I$ from a ring to its quotient is the map sending x to the coset $\bar{x}$. Note that π is surjective.

Proposition: Let R be a ring and I an ideal of R. Then the ideals of R/I are in bijection with the ideals of R which contain I.

Proof First pick an ideal $\bar{J}$ in R/I. Its pre-image $J = \pi^{-1}(\bar{J})$ is an ideal in R, since pre-images of ideals are again ideals. Moreover, it contains I since everything in I goes

to zero, and zero is in J. Conversely, suppose given an ideal J of R which contains I. Then we claim that $\pi(J)$ is an ideal in R/I. We know that it's an additive subgroup, since it's the image of a group homomorphism. It's closed under scaling: let $\bar{x} \in \pi(J)$, for some $x \in J$, and $\bar{y}$ be any other element of R/I. Since π is surjective, write $\bar{y} = \pi(y)$. Then $xy \in J$ (since it's an ideal), and $\pi(xy) = \overline{xy} = \bar{x}\bar{y}$, so $\bar{x}\bar{y}$ is in $\pi(J)$. To establish the bijection, we must check that $\pi(\pi^{-1}(\bar{J})) = \bar{J}$ and $\pi^{-1}(\pi(J)) = J$. I'll leave this to you...

Proposition: Let R be a ring.

1. An ideal $\mathfrak{p}$ is prime if and only if $R/\mathfrak{p}$ is an integral domain.
2. An ideal $\mathfrak{m}$ is maximal if and only if $R/\mathfrak{m}$ is a field.
3. Any maximal ideal is prime.

Proof 1. The condition for $\mathfrak{p}$ to be prime is "$ab \in \mathfrak{p}$ implies a or b is in $\mathfrak{p}$". In terms of the quotient ring $R/\mathfrak{p}$, this is exactly the same as saying "$\bar{a}\bar{b} = 0$ implies $\bar{a}$ or $\bar{b}$ is zero." This is exactly the statement that there cannot be zero divisors in $R/\mathfrak{p}$.

2. If $R/\mathfrak{m}$ is a field then the only ideals are $\langle 0\rangle$ and $R/\mathfrak{m}$. So the only ideals in R containing $\mathfrak{m}$ are their two pre images, namely $\mathfrak{m}$ and R. So $\mathfrak{m}$ is maximal. Conversely, if $\mathfrak{m}$ is maximal, then there are no ideals in $R/\mathfrak{m}$ containing $\langle 0\rangle$ besides $R/\mathfrak{m}$ itself. This means $\langle 0\rangle$ is the unique maximal ideal of $R/\mathfrak{m}$, which implies that everything outside $\langle 0\rangle$ is a unit (HW exercise), hence $R/\mathfrak{m}$ is a field. Alternatively, this implies $R/\mathfrak{m}$ has only two ideals, 0 and $R/\mathfrak{m}$ itself, so it is a field.

The relationship between prime and maximal ideals is as follows:

Warmup: Let R be a principal ideal domain, and $I = \langle a\rangle$ a nonzero ideal. Then I is prime if and only if I is maximal if and only if a is an irreducible element.

Radical ideals: Let R be a ring and $I \subseteq R$ an ideal. The **radical** of I, denoted by $\sqrt{I}$ or $\mathsf{Rad}(I)$, is the ideal

$$\sqrt{I} = \{x \in R : \exists n \in \mathbb{Z}^+; x^n \in I\}.$$

If $I = \sqrt{I}$, we say that I is a **radical ideal**.

Warmup: Show that $\sqrt{I}$ is the intersection of all the prime ideals containing I.

Example: Any prime ideal is radical. The ideal $6\mathbb{Z}$ is a radical ideal in $\mathbb{Z}$ and $\sqrt{12\mathbb{Z}} = 6\mathbb{Z}$.

1.1.11 Noetherian Rings

There is one more important property that polynomial rings $R[X]$ inherit from R: that of being noetherian.

Noetherian rings: A **noetherian ring** is a (commutative) ring with 1 in which every ascending chain of ideals terminates. In other words: if $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ is an ascending chain of ideals, then there is some index n such that $I_n = I_{n+1} = \ldots$.

Proposition: A ring R is Noetherian if and only if every ideal in R is finitely generated.

Proof Assume that R is Noetherian and let I be an ideal in R. If $I = \langle 0 \rangle$, we are done; if not, pick an element $a_1 \in I \backslash \langle 0 \rangle$. If $I = \langle a_1 \rangle$, we are done; if not, pick an element $a_2 \in I \backslash \langle a_1 \rangle$. If $I = \langle a_1, a_2 \rangle$, we are done; if not, pick $a_3 \in I \backslash \langle a_1, a_2 \rangle$ and continue. In this way we get an ascending chain of ideals

$$\langle a_1 \rangle \subsetneq \langle a_1, a_2 \rangle \subsetneq \ldots$$

Since R is Noetherian, this process must terminate, say at $\langle a_1, a_2, \ldots, a_n \rangle$, and then I is generated by $a_1, a_2, \ldots, a_n$.

Now assume that every ideal in R is finitely generated. Assume we have an ascending chain

$$I_1 \subsetneq I_2 \subsetneq \ldots$$

of ideals. Let I be the union of these I_j ; then I is an ideal, hence finitely generated, say $I = \langle a_1, a_2, \ldots, a_n \rangle$. Each of these elements lies in some I_j; let m be the maximal index occurring. Then $I \subseteq I_m$, hence $I_m = I_{m+1} = \ldots$.

As an immediate corollary we have

Corollary: Principal ideal domains are Noetherian.

Proof Exercise.

Theorem:(Hilbert basis theorem I) If R is a Noetherian ring, then so is the polynomial ring $R[x]$.

Proof Let I be an ideal in $R[x]$. We must show that I is finitely generated. For each non-negative integer n, let J_n be the ideal of R consisting of the leading coefficients of

polynomials in I whose degrees are less than or equal to n. Then

$$J_0 \subseteq J_1 \subseteq J_2 \subseteq \dots$$

is an ascending chain of ideals in the Noetherian ring R and, as such, must terminate, say, at J_k. So

$$J_0 \subseteq J_1 \subseteq \dots \subseteq J_k = J_{k+1} = \dots$$

Now, J_i is finitely generated for each $i = 1, 2, \dots, k$. Therefore, for each i, let $f_{i_1}, f_{i_2}, \dots, f_{i_r}$ be polynomials in $R[x]$ whose leading coefficients generate J_i in R. This gives us a finite set of polynomials, and it is not at all hard to see that this finite set of polynomials generates the ideal I. This completes the proof.

Warmup: Let K be a field, and let $x_1, x_2, \dots, x_n$ be n indeterminates. Then $K[x_1, x_2, \dots, x_n]$ is Noetherian.

1.2 Field Extensions

We begin with a simple but possibly surprising observation which makes fields rather interesting rings.

Proposition: If K and L are fields, then any homomorphism between them must be injective.

Proof Let $f : K \to L$ be a homomorphism. Then $\ker f$ is an ideal of K, and there are only two such: the zero and unit ideals. Note that $\ker f$ cannot be the unit ideal, or else f would be the zero map, which is not a homomorphism ($f(1) = 1$ for homomorphisms, and $1 \neq 0$ in a field). Thus $\ker f$ is trivial, so f is injective.

Field extensions: A **field extension** is an injective map $K \hookrightarrow L$ of fields. Equivalently (by identifying K with its image in L, which is a subring), it is a subring K of a field L which is also a field. In this situation, we will also speak of K being a **subfield of** L, or of L as an **extension of** K.

Example: (1) $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{2}] \subseteq \mathbb{R}$ and $\mathbb{R} \subseteq \mathbb{C}$ are all field extensions.
(2) For p prime, $\mathbb{Z}/p\mathbb{Z}$ is a field with p elements, which we will hereafter denote $\mathbb{F}_p$. The polynomial ring $\mathbb{F}_p[x]$ is not a field, but it is possible to find a polynomial $q(x)$ such that the quotient $\mathbb{F}_p[x]/\langle q(x)\rangle$ is also a field, in which case $\mathbb{F}_p \subseteq \mathbb{F}_p[x]/\langle q(x)\rangle$ is a field

extension.

(3) If K is a field, and x an indeterminate (or "formal") variable, the set $K(x) = \{\frac{p(x)}{q(x)} : q(x) \neq 0\}$ is a field; it is an extension of K (a very large one, as we will see). We say that $K(x)$ is the field obtained by **adjoining** x to the field K. This is different from the formation of $K[x]$, in which we adjoin the element x to form a new ring (the polynomial ring), which is not a field. The field $K(X)$ is often called the **field of rational functions** over K, to distinguish it from the polynomial ring. It's important to pay attention to the square brackets "[ ] " denoting "ring adjoin" and the parentheses "( )" denoting "field adjoin".

The degree of the extension: Let $K \subseteq L$ be a field extension. The **degree** of the extension, denoted $[L : K]$ is the dimension of L as a vector space over K. It may be infinite. We say that L is a finite extension (resp. infinite extension) of K to mean that its degree over K is finite (resp. infinite).

Example: (1) $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$, because the set $\{1, \sqrt{2}\}$ is a basis.

(2) $[\mathbb{C} : \mathbb{R}] = 2$, because $\{1, i\}$ is a basis.

(3) Let $\omega = e^{\frac{2\pi i}{3}}$, a **cube root of unity**. Then $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ because $\{1, \omega\}$ is a basis. Note that $1 + \omega + \omega^2 = 0$ (draw a picture...) so the set $\{1, \omega, \omega^2\}$ is linearly dependent.

(4) $[\mathbb{R} : \mathbb{Q}] = \infty$, because, for example, the set $\{\sqrt{p} : p \text{ is prime}\}$ is linearly independent (and infinite), and a finite-dimensional space cannot contain an infinite set of linearly independent elements.

(5) $K \subseteq K(x)$ is an infinite extension: the elements $1, x, x^2, \ldots$, are linearly independent.

Proposition: Let $K \subseteq L$ and $L \subseteq M$ be field extensions. Then in particular $K \subseteq M$ is also a field extension; it is finite if and only if $K \subseteq L$ and $L \subseteq M$ are both finite, in which case the degrees of the three extensions are related by the formula

$$[M : K] = [M : L][L : K].$$

Proof Let $[M : L] = m$ and $[L : K] = n$, and pick bases $a_1, \ldots, a_m$ for M over L and $b_1, \ldots, b_n$ for L over K. Then the set $\{a_i b_j : i = 1, \ldots, m, j = 1, \ldots, n\}$ is a basis for M over K (check).

Algebraic vs. Transcendental Extensions: Let $K \subseteq L$ be a field extension. An element $\alpha \in L$ is called **algebraic over** K if there is a nonzero polynomial $f \in K[x]$

such that $f(\alpha) = 0$. In this case we say that α **satisfies** or **is a root of** the polynomial f. If there is no such polynomial, α is called **transcendental** over K. If every element of L is algebraic over K, L is called an **algebraic field extension**. Otherwise it is called a **transcendental field extension**.

Example: (1) $\mathbb{Q}[\sqrt{2}]$ is an algebraic extension of $\mathbb{Q}$. Every element $a+b\sqrt{2}$ satisfies the polynomial relation $(a+b\sqrt{2})^2 - 2a(a+b\sqrt{2}) + (a^2-2b^2) = 0$, which is a rational polynomial.
(2) $\mathbb{Q}[\omega]$ is an algebraic extension of $\mathbb{Q}$, because the new element ω is algebraic over $\mathbb{Q}$; it is a root of $x^3 - 1$.
(3) $\mathbb{Q} \subseteq \mathbb{R}$ is a transcendental extension: for example, π is not algebraic over $\mathbb{Q}$.
(4) $\mathbb{C}$ is an algebraic extension of $\mathbb{R}$, essentially just because i satisfies the polynomial $x^2 + 1$.
(5) $K \subseteq K(x)$ is a transcendental extension: x does not satisfy any nonzero polynomial relation.

1.2.1 Algebraic Closures

If f is a polynomial of degree n over the rationals or the reals, or more generally over the complex numbers, then f need not have any rational roots, or even real roots, but we know that f always has n complex roots, counting multiplicity. This favorable situation can be duplicated for any field $\mathbb{F}$, that is, we can construct an algebraic extension C of $\mathbb{F}$ with the property that any polynomial in $C[X]$ splits over C. There are many ways to express this idea.

Proposition: If C is a field, the following conditions are equivalent.

1. Every nonconstant polynomial $f \in C[X]$ has at least one root in C.
2. Every nonconstant polynomial $f \in C[X]$ splits over C.
3. Every irreducible polynomial $f \in C[X]$ is linear.
4. C has no proper algebraic extensions.

Proof (1) implies (2): By (1) we may write $f = (X - \alpha)g$. Proceed inductively to show that any nonconstant polynomial is a product of linear factors.

(2) implies (3): If f is an irreducible polynomial in $C[X]$, then f is nonconstant.

By (2), f is a product of linear factors. But f is irreducible, so there can be only one such factor.

(3) implies (4): Let E be an algebraic extension of C. If $\alpha \in E$, let f be the minimal polynomial of α over C "the unique monic irreducible polynomial such that $f(\alpha) = 0$". Then f is irreducible and by (3), f is of the form $X - \alpha$. But then $\alpha \in C$, so $E = C$.

(4) implies (1): Let f be a nonconstant polynomial in $C[X]$, and adjoin a root α of f to obtain $C(\alpha)$. But then $C(\alpha)$ is an algebraic extension of C, so by (4), $\alpha \in C$.

Remark: If any (and hence all) of the conditions in previous proposition are satisfied, we say that C is **algebraically closed**.

It will be useful to embed an arbitrary field $\mathbb{F}$ in an algebraically closed field.

Algebraic closures: An extension C of $\mathbb{F}$ is an **algebraic closure** of $\mathbb{F}$ if C is algebraic over $\mathbb{F}$ and C is algebraically closed.

1.3 Problems

1. Let R be a commutative ring with unity. Prove that $\langle 0 \rangle$ is a prime ideal of R if and only if R is an integral domain.
2. A subset of a ring is said to be a **multiplicative system** if it is closed under multiplication and contains the multiplicative identity 1. Let R be a commutative ring with unity and P an ideal of R. Prove that P is a prime ideal if and only if $R \backslash P$ is a multiplicative system.
3. Let I and J be two ideals of a commutative ring with unity R, neither contained in the other. Prove that the ideal $I \cup J$ is not a prime ideal.
4. Let I be an ideal of a ring R, and let $a \in R$. Prove that the set
$$\{i + ra : i \in I \text{ and } r \in R\}$$
is an ideal of R. This ideal is denoted by $\langle I, a \rangle$ "the ideal generated by I and a".
5. Prove that every finite integral domain is a field.
6. Let R be a finite ring. Prove that any prime ideal of R is also a maximal ideal.
7. The **product of two ideals** I and J is defined to be the ideal generated by all

products ab, where $a \in I$ and $b \in J$. That is,if $S = \{ab : a \in I, b \in J\}$, then the product of I and J is given by

$$IJ = \langle S \rangle.$$

We can also view this product as all sums of such products

$$IJ = \{a_1b_1 + a_2b_2 + \ldots + a_nb_n : a_i \in I \text{ and } b_i \in J\}.$$

Let P be an ideal in a commutative ring with unity R. Prove that P is prime if and only if $IJ \subseteq P$ implies $I \subseteq P$ or $J \subseteq P$ for any ideals I and J of R.

8. Let D be a ring. Prove that D is an integral domain if and only if $D[x]$ is an integral domain. In particular, if K is a field, then $K[x]$ is an integral domain. Furthermore, D is an integral domain if and only if $D[x, y]$ is an integral domain. More generally, prove that D is an integral domain if and only if $D[x_1, x_2, \ldots, x_n]$ is an integral domain. Conclude that if K is a field, then $K[x_1, x_2, \ldots, x_n]$ is an integral domain.
9. Recall the **Zorn's lemma**: Let $\preceq$ be a partial order on a non-empty set S. If every chain in S has an upper bound in S, then S contains a maximal. Show that every nonzero ring has at least one maximal ideal.
10. Use Zorn's lemma to prove that every proper ideal of a ring is contained in a maximal ideal. (Hint: let I be an ideal of a ring R; the key is to choose carefully a set S of ideals such that when Zorn's lemma gives you a maximal element of S, this will turn out to be a maximal ideal containing I.)
11. Let R be a commutative ring with unity. Prove that the union of all the maximal ideals of R is the set of non-units of R:

$$\bigcup_{\mathfrak{m} \in \mathsf{MaxSpec}(R)} \mathfrak{m} = R \backslash R^{\times}.$$

12. Prove that the nilradical of a commutative ring with unity R is the intersection of all prime ideals in R — that is

$$\bigcap_{\mathfrak{p} \in \mathsf{Spec}(R)} \mathfrak{p} = \mathsf{Nil}(R).$$

13. Let x be an element of a unique factorization domain D. Prove that x is prime if and only if x is irreducible.
14. Let R be the ring of all polynomials with integer coefficients that have no x term; that is, all polynomials of the form

$$a_0 + a_2x^2 + a_3x^3 + \ldots + a_nx^n.$$

This particular polynomial ring is usually denoted by $R = \mathbb{Z}[x^2, x^3]$. Find $\gcd(x^2, x^3)$ and $\gcd(x^5, x^6)$ in R. Also, show that R is not a unique factorization domain.

15. Show that in any principal ideal domain, every nonzero prime ideal is a maximal ideal.
16. Let D be a principal ideal domain. Prove that, for an element $x \neq 0 \in D$, x is irreducible if and only if $\langle x \rangle$ is maximal.
17. Let K be a field. Find $\mathsf{Spec}(K[x])$ and $\mathsf{MaxSpec}(K[x])$.
18. Let $f : R \to S$ be an onto homomorphism between two rings R and S. Show that if an ideal I of R is finitely generated, then its homomorphic image $f(I)$ is also finitely generated.
19. Prove that any homomorphic image of a Noetherian ring is Noetherian —that is, prove that if I is an ideal of a Noetherian ring R, then R/I is also Noetherian.

Chapter 2 Basic Algebraic geometry

2.1 What is Algebraic Geometry?

Algebraic Geometry is the study of the geometry of the set of common zeros of a collection of polynomials.

Recall: If R is a commutative ring, then $R[X_1, \ldots, X_n]$ is a commutative ring.

Affine n-space: $\mathbb{A}^n_R = \mathbb{A}^n = R^n = \{(r_1, \ldots, r_n) : r_i \in R\}$.

Polynomial map: Every $f \in R[X_1, \ldots, X_n]$ defines a polynomial map $f : \mathbb{A}^n_R \to R, a \mapsto f(a)$.

Affine algebraic set: $\mathbb{V}_R(S) = \mathbb{V}(S) = \{a \in R^n : f(a) = 0 \text{ for all } f \in S\}$ for some $S \subseteq R[X_1, \ldots, X_n]$.

Remark: We write $\mathbb{V}(S) = \mathbb{V}(f_1, \ldots, f_k)$ if $S = \{f_1, \ldots, f_k\}$.

Example: $\mathbb{V}_{\mathbb{R}}(X^2 + Y^2 - 1) = \{(a, b) \in \mathbb{R}^2 : a^2 + b^2 = 1\} \neq \emptyset$ (infinite set).

$\mathbb{V}_{\mathbb{Q}}(X^2 + Y^2 - 1) = \{(a, b) \in \mathbb{Q}^2 : a^2 + b^2 = 1\} \neq \emptyset$ (countable set).

$\mathbb{V}_{\mathbb{F}_2}(X^2 + Y^2 - 1) = \{(a, b) \in \mathbb{F}_2^2 : a^2 + b^2 = 1\} \neq \emptyset$ (finite set).

$\mathbb{V}_{\mathbb{Z}}(X^2 + Y^2 - 1) = \{(a, b) \in \mathbb{Z}^2 : a^2 + b^2 = 1\} = \{(\mp 1, 0), (0, \mp 1)\}$ (finite set).

$\mathbb{V}_{\mathbb{R}}(X^2 + Y^2 + 1) = \{(a, b) \in \mathbb{R}^2 : a^2 + b^2 = -1\} = \emptyset$ (empty set).

$\mathbb{V}_{\mathbb{C}}(X^2 + Y^2 - 1) = \{(a, b) \in \mathbb{C}^2 : a^2 + b^2 = -1\} \neq \emptyset$.

Example: Let c be a constant polynomial in $R[X_1, \ldots, X_n]$. Then $\mathbb{V}_R(c) = R^n$ if $c = 0$, and $\mathbb{V}_R(c) = \emptyset$ if $c \neq 0$. In particular, $\mathbb{V}_R(1) = \emptyset$.

Example: Consider $Y - X^2, Y^2 - X^3, Y^2 - (X^3 + X^2)$ in $\mathbb{R}[X, Y]$. Then

$$\mathbb{V}_{\mathbb{R}}(Y - X^2) = \text{ affine plane curve which is a conic.}$$

$$\mathbb{V}_{\mathbb{R}}(Y^2 - X^3) = \text{ affine plane curve which is a cuspidal cubic.}$$

$$\mathbb{V}_{\mathbb{R}}(Y^2 - (X^3 + X^2)) = \text{ affine plane curve which is a nodal cubic.}$$

Example: In this example we show that $\mathbb{V}_R(f_1,\dots,f_k) = \bigcap_{j=1}^k \mathbb{V}_R(f_j)$ for any $f_1,\dots,f_k \in R[X_1,\dots,X_n]$. Note that

$$\begin{aligned} a \in \mathbb{V}_R(f_1,\dots,f_k) &\Leftrightarrow f_j(a) = 0 \text{ for all } j = 1,\dots,k \\ &\Leftrightarrow a \in \mathbb{V}_R(f_j) \text{ for all } j = 1,\dots,k \\ &\Leftrightarrow a \in \bigcap_{j=1}^k \mathbb{V}_R(f_j). \end{aligned}$$

Warmup: For any collection $\mathcal{C} = \{f_\lambda : \lambda \in \Lambda\} \subseteq R[X_1,\dots,X_n]$, we have

$$\mathbb{V}_R(\mathcal{C}) = \bigcap_{\lambda\in\Lambda} \mathbb{V}_R(f_\lambda).$$

Example: In this example we show that $\mathbb{V}_R(f_1\dots f_k) = \bigcup_{j=1}^k \mathbb{V}_R(f_j)$ for any $f_1,\dots,f_k \in R[X_1,\dots,X_n]$. Note that

$$\begin{aligned} a \in \bigcup_{j=1}^k \mathbb{V}_R(f_j) &\Rightarrow f_j(a) = 0 \text{ for some } j = 1,\dots,k \\ &\Rightarrow a \in (f_1\dots f_k)(a) = f_1(a)\dots f_k(a) = 0 \\ &\Rightarrow a \in \mathbb{V}_R(f_1\dots f_k). \\ a \notin \mathbb{V}_R(f_1\dots f_k) &\Rightarrow (f_1\dots f_k)(a) = f_1(a)\dots f_k(a) \neq 0 \text{ for all } j = 1,\dots,k \\ &\Rightarrow f_j(a) \neq 0 \text{ for all } j = 1,\dots,k \\ &\Rightarrow a \notin \mathbb{V}_R(f_j) \text{ for all } j = 1,\dots,k \\ &\Rightarrow a \notin \bigcup_{j=1}^k \mathbb{V}_R(f_j). \end{aligned}$$

Proposition: Let $S \subseteq T$ in $R[X_1,\dots,X_n]$. Then $\mathbb{V}_R(T) \subseteq \mathbb{V}_R(S)$.

Proof Suppose that $S \subseteq T$ in $R[X_1,\dots,X_n]$. Then

$$\begin{aligned} a \in \mathbb{V}_R(T) &\Rightarrow f(a) = 0 \text{ for all } f \in T \\ &\Rightarrow f(a) = 0 \text{ for all } f \in S \ (S \subseteq T) \\ &\Rightarrow a \in \mathbb{V}_R(S). \end{aligned}$$

Example: Given $S = \{Y - \sqrt{2}, X^2 + Y^2 - 4\} \subseteq \{Y - \sqrt{2}, X^2 + Y^2 - 4, X - \sqrt{2}\}$ in $\mathbb{R}[X,Y]$. Then $\mathbb{V}_R(T) = \{(\sqrt{2},\sqrt{2})\} \subseteq \{(\sqrt{2},\sqrt{2}),(-\sqrt{2},\sqrt{2})\} \subseteq \mathbb{V}_R(S)$.

Proposition: Let $S_1,\dots,S_k \subseteq R[X_1,\dots,X_n]$. Let $\{S_\lambda : \lambda \in \Lambda\}$ be a collection of subsets in $R[X_1,\dots,X_n]$. Then

1. $\mathbb{V}_R(S_1\dots S_k) = \bigcup_{j=1}^k \mathbb{V}_R(S_j)$;
2. $\mathbb{V}_R(\bigcup_{\lambda\in\Lambda} S_\lambda) = \bigcap_{\lambda\in\Lambda} \mathbb{V}_R(S_\lambda)$,

where $S_1 \dots S_k = \{f_1 \dots f_k : f_j \in S_j, j = 1, \dots, k\}$.

Proof Let $j \in \{1, \dots, k\}$ and $a \in \mathbb{V}_R(S_j)$, then $f(a) = 0$ for all $f \in S_j$. Moreover, each product $f_1 \dots f_k$ contains one factor f in S_j, and hence each product vanishes at a. Thus, $\mathbb{V}_R(S_j) \subseteq \mathbb{V}_R(S_1 \dots S_k)$ for all $j \in \{1, \dots, k\}$. Thus, $\bigcup_{j=1}^{k} \mathbb{V}_R(S_j) \subseteq \mathbb{V}_R(S_1 \dots S_k)$. Now, suppose that $a \in \mathbb{V}_R(S_1 \dots S_k)$ and $a \notin \mathbb{V}_R(S_j)$ for all $j = 1, \dots, k$. Then, for every $j \in \{1, \dots, k\}$ there is $g_j \in S_j$ such that $g_j(a) \neq 0$. It follows that $g_1 \dots g_k \in S_1 \dots S_k$ and $g_1 \dots g_k(a) \neq 0$ which is contradiction. Finally, we prove (2):

$$
\begin{aligned}
S_\lambda \subseteq \bigcup_{\lambda\in\Lambda} S_\lambda \text{ for all } \lambda \in \Lambda &\Rightarrow \mathbb{V}_R(\bigcup_{\lambda\in\Lambda} S_\lambda) \subseteq \mathbb{V}_R(S_\lambda) \text{ for all } \lambda \in \Lambda. \\
&\Rightarrow \mathbb{V}_R(\bigcup_{\lambda\in\Lambda} S_\lambda) \subseteq \bigcap_{\lambda\in\Lambda} \mathbb{V}_R(S_\lambda) \\
a \in \bigcap_{\lambda\in\Lambda} \mathbb{V}_R(S_\lambda) &\Rightarrow f(a) = 0 \text{ for all } \lambda \in \Lambda \text{ and } f \in S_\lambda \\
&\Rightarrow f(a) = 0 \text{ for all } f \in \bigcup_{\lambda\in\Lambda} S_\lambda \\
&\Rightarrow a \in \mathbb{V}_R(\bigcup_{\lambda\in\Lambda} S_\lambda).
\end{aligned}
$$

Proposition: Let $S \subseteq R[X_1, \dots, X_n]$. Then $R[X_1, \dots, X_n]$. Then $\mathbb{V}_R(S) = \mathbb{V}_R(\langle S \rangle)$, where $\langle S \rangle$ is the ideal generated by S.

Proof It is clear that $\mathbb{V}_R(\langle S \rangle) \subseteq \mathbb{V}_R(S)$ since $S \subseteq \langle S \rangle$. Now, if $a \in \mathbb{V}_R(S)$ then $f(a) = 0$ for all $f \in S$. So, every R-linear combination in $\langle S \rangle$ will be vanished at a. Hence, $\mathbb{V}_R(S) \subseteq \mathbb{V}_R(\langle S \rangle)$.

Remark: We can rewrite the previous results on the vanishing sets in terms of ideals of $R[X_1, \dots, X_n]$. Let $\{I, J, I_1, \dots, I_k\}$, and $\{I_\lambda : \lambda \in \Lambda\}$ are collections of ideals in $R[X_1, \dots, X_n]$. Then

- $\mathbb{V}_R(\mathbf{0}) = R^n$, where $\mathbf{0} = \langle 0 \rangle$ is the zero ideal,
- $\mathbb{V}_R(\mathbf{1}) = \emptyset$, where $\mathbf{1} = \langle 1 \rangle$,
- $\mathbb{V}_R(I_1 \dots I_k) = \bigcup_{j=1}^{k} \mathbb{V}_R(I_j)$. Here, $I_1 \dots I_k$ is all finite sum $\sum_{\text{finite}} f_1 \dots f_k$, where $f_j \in I_j, j = 1, \dots, k$.
- $\mathbb{V}_R(\bigcup_{\lambda\in\Lambda} I_\lambda) = \bigcap_{\lambda\in\Lambda} \mathbb{V}_R(I_\lambda)$.

A topology on a set: A **topology** on a set X is a collection of distinguished subsets, called closed sets, satisfying:

1. $\emptyset$ and X are closed.

2. An arbitrary intersection of closed sets is closed.
3. A finite union of closed sets is closed.

Example (1) On $\mathbb{R}$, the Euclidean topology.
(2) On $\mathbb{R}$, cofinite topology: closed sets are finite sets, and $\mathbb{R}$; $\emptyset$.

The Zariski topology: The **Zariski topology** on k^n (here k is algebraically closed field) is defined as the topology whose closed sets are affine algebraic sets.

Warmup: Let $S = \{f_\lambda\}_{\lambda\in\Lambda} \subseteq R[X_1, \ldots, X_n]$ and let $I \subseteq R[X_1, \ldots, X_n]$ be the ideal generated by the $\{f_\lambda\}_{\lambda\in\Lambda}$. Prove that $\mathbb{V}_R(S) = \mathbb{V}_R(I)$. In particular, if k is an algebraically closed field and $S \subseteq k[X_1, \ldots, X_n]$, then there is $f_1, f_2, \ldots, f_r \in k[X_1, \ldots, X_n]$ such that $\mathbb{V}_k(S) = \mathbb{V}_k(f_1, f_2, \ldots, f_r)$.

Theorem:(Hilbert basis theorem II). Every affine algebraic set in k^n, where k is an algebraically closed field, can be defined by finitely many polynomials.

Proof Apply the exercise above.

IMPORTANT: For the remainder of these lectures, all fields will be assumed algebraically closed field, without further mention, unless explicitly stated otherwise.

Ideal of an affine algebraic set: An affine algebraic subset of k^n is a set

$$V = \mathbb{V}_k(\langle f_1, f_2, \ldots, f_r\rangle) = \mathbb{V}_k(f_1, f_2, \ldots, f_r) \subseteq k^n.$$

Consider the map

$$\{\text{ideals in } k[X_1, \ldots, X_n]\} \longrightarrow \{\text{(affine) algebraic subsets of } k^n\}$$
$$I \longmapsto \mathbb{V}_k(I)$$

- This map is order reversing: $I \subseteq J \Longrightarrow \mathbb{V}_k(I) \supseteq \mathbb{V}_k(J)$.
- Surjective.
- Not injective: e.g., $\langle x, y\rangle$; $\langle x^2, y^2\rangle$.

Proposition: Let $I \subseteq k[X_1, \ldots, X_n]$. Then $\mathbb{V}_k(I) = \mathbb{V}_k(\sqrt{I})$.

Proof $I \subseteq \sqrt{I} \Longrightarrow \mathbb{V}_k(\sqrt{I}) \subseteq \mathbb{V}_k(I)$. So take $p \in \mathbb{V}_k(I) \subseteq k^n$. Need to show for all $f \in \sqrt{I}$ that $f(p) = 0$. We have $f \in \sqrt{I}$ implies $f^m \in I$ for some positive integer m, so

$$(f(p))^m = f^m(p) = 0 \Longrightarrow f(p) = 0.$$

Now is the map $I \longrightarrow \mathbb{V}_k(I)$ injective?

Example: Consider the two ideals $\langle x^2+y^2\rangle, \langle x, y\rangle$ in $\mathbb{R}[x, y]$. We have 2 radical ideals defining the same algebraic set:

$$\mathbb{V}_k(\langle x, y\rangle) = \{(0, 0)\} = \mathbb{V}_k(\langle x^2+y^2\rangle) \subseteq \mathbb{R}^2.$$

Ideal of an algebraic set: Let $V \subseteq k^n$ be an affine algebraic set. The **ideal of** V is

$$\mathbb{I}(V) = \{f \in k[X_1, \ldots, X_n] : f(p) = 0 \text{ for all } p \in V\}.$$

Proposition: $\mathbb{I}(V)$ is a radical ideal, and is the largest ideal defining V. Moreover, $V = \mathbb{V}(\mathbb{I}(V))$ and hence $\mathbb{I}$ is a right inverse of $\mathbb{V}$.

Proof Say $V = \mathbb{V}(I)$. Since $I \subseteq \mathbb{I}(V)$, we have $\mathbb{V}(\mathbb{I}(V)) \subseteq \mathbb{V}(I) = V$. Now, take $p \in V$. Need to show that for all $g \in \mathbb{I}(V)$, $g(p) = 0$, which is true by definition of $\mathbb{I}(V)$.

Hilbert's Nullstellensatz: