1 The Integers, $k[x]$: Foundations and Big Questions

This section summarizes 5 key theorems about the integers, and their analogues for the polynomial ring $k[x]$ over a field k. It elaborates on other analogous results between $\mathbb{Z}$ and $k[x]$ including some major conjectures about the integers.

Key properties of the integers

Theorem 1.1 (Quotient-Remainder)**.** *Let a and b be integers with $b > 0$. There exist unique integers q, r such that*

(1) $a = bq + r$, and

(2) $0 \leq r < b$

Theorem 1.2 (GCD)**.** *Let a and b be integers, at least one of them nonzero. The gcd of a and b is the smallest positive linear combination of a and b. In particular, $\gcd(a, b) = au + bv$ for some integers u and v.*

The set of all linear combinations of a and b equals the set of multiples of $\gcd(a, b)$.

There is an efficient algorithm to compute the gcd of two integers.

Theorem 1.3 (Euclidean Algorithm)**.** *Let a, b be integers with $b \neq 0$. The following algorithm outputs $\gcd(a, b)$ in at most $1 + \log_2 b / \log \alpha$ steps, where $\alpha = (1+\sqrt{5})/2$ is the golden ratio. The Extended Euclidean Algorithm outputs integers u, v with $|u| < b$ and $|v| < a$ such that $au + bv = \gcd(a, b)$.*

Let's assume $a \geq b \geq 0$. Set $r_{-1} = a$ and $r_0 = b$, and define inductively q_k and r_{k+1} by applying the Quotient-Remainder Theorem to r_{k-1} and r_k (while $r_k \neq 0$), so $r_k = r_{k-1}q_k + r_{k+1}$.

$$\begin{aligned} q_k &= r_{k-1}//r_k && \text{the integer quotient} \\ r_{k+1} &= r_{k-1}\%r_k, && \text{the remainder} \\ r_{k+1} &= r_{k-1} - q_k r_k \end{aligned}$$

The r_k are a strictly decreasing sequence of nonnegative integers, so the process must terminate: for some n, $r_{n+1} = 0$. The following lemma shows that

$$\gcd(a, b) = \gcd(b, r_1) = \cdots = \gcd(r_n, r_{n+1}) = \gcd(r_n, 0) = r_n$$

Lemma 1.4. *For integers a, b, c, s such that $a = bs + c$, we have $\gcd(a, b) = \gcd(b, c)$.*

In the following Sage code we only keep two of the remainders at any time, not the whole sequence: after the kth pass through the while loop, r in the algorithm is r_{k-1} and s is r_k.

```
def euclid_alg(a,b):
   if b == 0:
      print "division by zero"
      return false
   else:
      r = a
      s = b
      while s != 0:
         rem =  r %s
         r = s
         s = rem
      return r
```

The Extended Euclidean algorithm produces two integers u, v such that $au + bv = \gcd(a, b)$. I like the following matrix version of the algorithm. Let

$$Q_k = \begin{bmatrix} -q_k & 1 \\ 1 & 0 \end{bmatrix} \qquad \text{and} \qquad R_k = \begin{bmatrix} r_k \\ r_{k-1} \end{bmatrix}$$

where the sequence r_k and q_k are the same as used above in the Euclidean algorithm. The following exercise finishes the discussion.

Exercises 1.5. Show that the Extended Euclidean Algorithm produces a linear combination of a and b that gives $\gcd(a, b)$.

(a) Verify that $R_{k+1} = Q_k R_k$.

(b) Let $R_0 = \begin{bmatrix} b \\ a \end{bmatrix}$. Show that $R_{n+1} = \begin{bmatrix} 0 \\ r_n \end{bmatrix} = Q_n Q_{n-1} \cdots Q_0 R_0$.

(c) Let $M = Q_n Q_{n-1} \cdots Q_0$. Show that $M_{2,1} b + M_{2,2} a = r_n = \gcd(a, b)$.

(d) Show that the determinant of M is ± 1.

Definition 1.6. Let r be an integer with $|r| > 1$. We say r is **irreducible** when $r = ab$ implies that either $a = \pm 1$ or $b = \pm 1$ (and the other is $\pm p$). We say r is **prime** when $r|ab$ implies $r|a$ or $r|b$.

Theorem 1.7 (Prime-Irreducible)**.** *A nonzero integer is irreducible if and only it is prime.*

The previous theorem is the key ingredient to establishing unique factorization.

Theorem 1.8 (Unique Factorization)**.** *Let a be a nonzero integer. There is a non-negative integer t, positive prime numbers $p_1, \ldots, p_t$, and positive integers $e_1, \ldots e_t$ and choice of unit, $u = 1$ or -1, such that*

$$a = up_1^{e_1} \cdots p_t^{e_t}$$

Each of t, p_i, e_i and u is uniquely determined up to reordering of the $p_i^{e_i}$.

KEY PROPERTIES OF $k[x]$

Theorem 1.9 (Quotient-Remainder)**.** *Let $a(x)$ and $b(x)$ be in $F[x]$ with $b(x) \neq 0$. There exist unique $q(x)$, $r(x)$ such that*

(1) $a(x) = b(x)q(x) + r(x)$, and

(2) $\deg r(x) < \deg b(x)$

Theorem 1.10 (GCD)**.** *Let $a(x), b(x) \in F[x]$ with at least one of them nonzero. There is a unique polynomial $d(x)$ satisfying*

(1) $d(x)$ is a common divisor of $a(x)$ and $b(x)$,

(2) $d(x)$ is monic,

(3) $d(x)$ is divisible by all other common divisors of $a(x)$ and $b(x)$ (so it is the greatest common divisor).

Furthermore, there exist $u(x), v(x) \in F[x]$ such that $d(x) = a(x)u(x) + b(x)v(x)$. The set of all polynomial combinations of $a(x)$ and $b(x)$ equals the set of multiples of $d(x)$.

The discussion of the Euclidean algorithm for integers carries over almost verbatim to the polynomial ring. Assume $\deg(a(x)) \geq \deg(b(x))$. Set $r_{-1}(x) = a(x)$ and $r_0(x) = b(x)$, and define inductively (while $r_k(x) \neq 0$)

$$\begin{aligned} q_k(x) &= r_{k-1}(x)//r_k(x) \\ r_{k+1}(x) &= r_{k-1}(x)\%r_k(x), \quad \text{so that} \\ r_{k+1}(x) &= r_{k-1}(x) - q_k(x)r_k(x) \end{aligned}$$

Then $\deg(r_k(x))$ is a sequence of polynomials of strictly decreasing degree so the process must terminate: for some n, $r_{n+1}(x) = 0$ and r_n is the gcd of $a(x)$ and $b(x)$.

Theorem 1.11 (Prime-Irreducible)**.** *Any nonconstant element of $F[x]$ is irreducible if and only if it is prime.*

Theorem 1.12 (Unique Factorization)**.** *Let $a(x) \in F[x]$ be nonzero. There is a nonnegative integer t, a constant $u \in F$, distinct monic irreducible polynomials $p_1(x), \ldots, p_t(x)$, and positive integers $e_1, \ldots e_t$ such that*

$$a(x) = u\big(p_1(x)\big)^{e_1}\big(p_2(x)\big)^{e_2}\cdots\big(p_t(x)\big)^{e_t}$$

Each of t, $p_i(x)$, e_i and u is uniquely determined, up to reordering of the $\big(p_i(x)\big)^{e_i}$.

The analogies between $\mathbb{Z}$ and $k[x]$

The fundamental theorems listed above show that there are strong parallels between the integers and the univariate polynomial ring over a field. It extends to the comparison of number fields and function fields of curves.

Definition 1.13. Let $D = \mathbb{Z} \setminus \{0\}$. The **rational numbers** are $\mathbb{Q} = D^{-1}\mathbb{Z}$. A **number field** is a finite extension of the rational numbers. Each number field K is defined (although not uniquely) by an irreducible polynomial $m(x) \in \mathbb{Q}[x]$. $K = \mathbb{Q}[x]/m(x)$.

Definition 1.14. Let k be a field and let $D = k[x] \setminus \{0\}$. The **rational polynomials** are $k(x) = D^{-1}(k[x])$. A **curve** is defined by a polynomial in y with coefficients in $k(x)$ that is irreducible. The **function field** of the curve defined by $m(y) = a_n(x)y^n + a_{n-1}(x)y^{n-1} + \cdots + a_1(x)y + a_0(x)$ is

$$K = k(x)[y]/m(y)$$

The field $k(x)$ is itself a function field. Here is another example.

Example 1.15. Let $m(y) = y^3 - (x^3 - x)$. Trust me, this is irreducible (you can use Eisenstein's criteria as we will see later). The function field from $m(y)$ is

$$K = k(x)[y]/y^3 - (x^3 - x))$$

Each element of K is uniquely represented as a polynomial in y of degree at most 2 with coefficients from $k(x)$.

The analogy between number fields and function fields of curves is particularly strong for the specific case when the base field is finite.

Riemann Hypothesis

The Riemann zeta function is a very important tool in analytic number theory that is related to the distribution of prime numbers. More specifically, through

various transformations it gives information about the number of primes less than a given integer.

$$\begin{aligned}\zeta(s) &= \sum_{n=1}^{\infty} \frac{1}{n^s} \\ &= \prod_{p \text{ prime}} (1 + p^{-s} + p^{-2s} + p^{-3s} + \cdots) \\ &= \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}\end{aligned}$$

The Riemann zeta function can be extended to the complex plane through analytic continuation, and it has poles at the even negative integers. The **Riemann hypothesis** states that the only other poles are at complex numbers s with $\mathrm{Re}(s) = 1/2$. This has implications for the distribution of primes, but they are not easy to spell out succinctly.

The relationship to the distribution of primes, the analytic continuation of ζ, and related topics are well beyond what we will study, but the interesting thing is that there are analogous zeta functions for $\mathbb{F}_q[x]$. In fact, number theorists consider not only the zeta function above but the generalized zeta functions for number fields (algebraic extensions of the rational numbers). The Weil conjectures are the geometric analogue. They deal with zeta functions for curves (and projective varieties of higher dimension) over finite fields.

The rather amazing thing is that the Weil conjectures, including the analogue of the Riemann hypothesis, have been proven, while the original Riemann hypothesis has not been proven.

The *abc* conjecture

Definition 1.16. Let n be an integer with unique factorization $n = up_1^{e_1}p_2^{e_2}\cdots p_t^{e^t}$. The **radical** of n is the square free positive integer $\mathrm{rad}(n) = p_1p_2\cdots p_t$.

The *abc* conjecture is relatively simple to state. From a very high level one can say that it relates the sum of two numbers with the factorizations of the two numbers and of their sum.

Conjecture 1.17 (abc)**.** *Let $\epsilon > 0$. There exist only finitely many triples of coprime positive integers a, b, c with $c = a + b$ such that*

$$c > \mathrm{rad}(abc)^{1+\epsilon}$$

One way to gain intuition about this conjecture is to take the extreme case when a and b are large powers of a small prime (or a small number of small primes). The conjecture says that the situations in which the sum $a + b$ is also a product of small primes is very rare.

Example 1.18. Suppose $a = 2^s$ and $b = 3^t$. Let's take $\epsilon = 1$ (the conjecture is interesting as ϵ goes to zero, but 1 is adequate for this example.) Let $c = 2^s + 3^t$ and factor $c = p_1^{e_1} p_2^{e_2} \cdots p_t^{e^t}$ with each $e_i \geq 1$. Note that none of the p_i is equal to 2 or 3. The conjecture states that except for a finite number of cases

$$2^s + 3^t < \big(2 \cdot 3 \cdot \operatorname{rad}(2^s + 3^t)\big)^2$$

Simplifying the right hand side and substituting for c,

$$p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t} < 36(p_1 p_2 \cdots p_t)^2$$

Consequently,

$$p_1^{e_1-2} p_2^{e_2-2} \cdots p_t^{e_t-2} < 36$$

Note that some of the $e_i - 2$ may be negative so it is hard to draw more specific conclusions. You will in an exercise.

There is an analogous statement for the polynomial ring $k[x]$. In place of an inequality about the size of integers we have an inequality about the degree of polynomials. The **radical** is defined in analogy to the radical of an integer.

$$\operatorname{rad}\Big(u\big(p_1(x)\big)^{e_1}\big(p_2(x)\big)^{e_2} \cdots \big(p_t(x)\big)^{e_t}\Big) = p_1(x)p_2(x)\cdots p_t(x)$$

This theorem has been proven, and it is not difficult to prove, so we will do it later in the course.

Theorem 1.19 (Mason-Stothers)**.** *Let $a(x)$, $b(x)$, and $c(x)$ be coprime polynomials over a field k such that $a(x)+b(x) = c$ and such that not all of them have vanishing derivative. Then*

$$\max\{\deg(a(x)), \deg(b(x)), \deg(c(x))\} \leq \deg\big(\operatorname{rad}(a(x)b(x)c(x))\big) - 1.$$

Fermat's last theorem

Fermat's last theorem became an actual theorem in 1995, many years after it was proposed in 1637.

Theorem 1.20 (Fermat-Wiles)**.** *For an integer $n \geq 3$. There is no triple of positive integers a, b, c such that $a^n + b^n = c^n$.*

The proof of this result definitely does not fit in the margin of a piece of paper. Wiles used sophisticated algebra, number theory and algebraic geometry to prove it.

There is an analogue for polynomials over a field

Theorem 1.21. *Let k be a field of characteristic 0 and let $n \geq 3$ be an integer. Suppose that $a(x)$, $b(x)$, and $c(x)$ are three coprime polynomials in $k(x)$ satisfying $a(x)^n + b(x)^n = c(x)^n$. Then all three polynomials are constants.*

The result can be extended to the case of finite characteristic, but that requires a subtle additional restriction. The proof of the result for polynomials is one of your assigned problems.

Why?

We have just listed three conjectures for the integers (well, one, Fermat's last theorem is now proven) that have analogues for polynomials that are proven. Two of the polynomial theorems are within our ability to prove. What makes the polynomial versions easier than the integer versions?

Assignment 1: Due Thursday 1/26.

Do Exercise 1.5 on your own.

Exercises 1.22. Let R be an integral domain. We would like to formulate a Quotient-Remainder Theorem and a Euclidean Algorithm for $R[x]$.

- **(a)** Show that the Quotient-Remainder theorem holds with no change, provided the divisor is monic.
- **(b)** In $\mathbb{Z}[x]$ let $f(x) = 3x^3 + 5x^2 + x + 6$ and $g(x) = 2x + 5$. Show that there is a integer m, a $Q(x) \in \mathbb{Z}[x]$ and an $R \in \mathbb{Z}$ such that $mf(x) = g(x)Q(x) + R$. What is special about m? What kind of uniqueness statement can you make?.
- **(c)** Same exercise with $g(x) = 3x^2 + 2x + 1$.
- **(d)** With these exercises as motivation, can you formulate a QR theorem for an arbitrary $R[x]$ with R an integral domain?

Exercises 1.23. We consider positive integers s, t and c such that $2^s + 3^t = c$.

(a) Assuming the *abc* conjecture, show that there are only a finite number of such triples satisfying $c/\operatorname{rad}(c) > 7(\operatorname{rad}(c))^{\epsilon}$.

Exercises 1.24.

(a) Use the Mason-Stother theorem to prove the analogue of Fermat's last theorem for polynomials. To make the proof simpler, assume (WLOG) that $a(x)$ has degree $\geq$ to the degrees of $b(x)$, $c(x)$.

2 Geometry and Polynomials

Let k be a field. One important difference between polynomials and integers is that each polynomial in $k[x]$ can be considered as a function: it determines a function from k to k. Let $f(x) \in k[x]$ with $f(x) = f_n x^n + f_{n-1}x^{n-1} + \cdots + f_1 x + f_0$. The function defined by $f(x)$ is

$$\begin{aligned} f : k &\longrightarrow k \\ a &\longmapsto f(a) = f_n a^n + f_{n-1}a^{n-1} + \cdots + f_1 a + f_0 \end{aligned}$$

We can think about this geometrically by "graphing" the function in k^2. (For $k = \mathbb{R}$ this is the usual notion of graphing, but for $\mathbb{C}$ or finite fields we will have to be more schematic.)

We explore and expand on this geometry in this section. We also make use of the universal property of polynomial rings.

Theorem [Universal Property of $k[x]$] Let k be contained in some ring R. For any $a \in R$ there is a unique homomorphism from $k[x]$ to R that takes x to a, namely

$$\begin{aligned} \varphi_a : k[x] &\longrightarrow R \\ \sum_i f_i x^i &\longmapsto \sum_i f_i a^i \end{aligned}$$

This map will be called the **evaluation at** a homomorphism.

It is important to observe the distinction between the two functions we have just introduced. The first: given an $f(x) \in k[x]$ we have a function that takes k to k that evaluates a *fixed* $f(x)$ at *all* elements of k. It is not a homomorphism (except for a very special case). The second: given $a \in k$ there is a homomorphism from $F[x]$ to k. It evaluates *all* $f(x)$ at a *fixed* $a \in k$.

The Roots-Factors Theorem

Let's now think of a fixed $f(x)$ and the graph of $f(x)$ in k^2. That is, in the x-y plane the points $(x, f(x))$ form the graph of $f(x)$. The intersection of this graph with the line $y = 0$ is the set of roots of $f(x)$.

Definition 2.1. Let $f(x) \in k[x]$. An element $a \in k$ is a **root** of $f(x)$ when $f(a) = 0$.

Theorem 2.2. *Let $f(x) \in k[x]$. Then a is a root of $f(x)$ if and only if $(x - a)$ is a factor of $f(x)$. Consequently, if $f(x)$ has degree n then f has at most n distinct roots.*

Proof. From the Quotient-Remainder theorem $f(x) = (x-a)q(x)+r(x)$ for unique polynomials $q(x)$ and $r(x)$. We also have $\deg(r(x)) < \deg(x-a)$ so $r(x)$ is actually a constant, $r \in k$. Now appy the evaluate at a homomorphism. We get

$$f(a) = (a-a)q(a) + r = r$$

In particular, a is a root of $f(x)$ if and only if $f(a) = 0$, which is true if and only if $r = 0$.

If $f(x)$ has t distinct roots, $a_1, \ldots, a_t$, then it has t distinct factors $(x - a_i)$ for $i = 1, \ldots, t$. Then, by unique factorization, $(x - a_1)(x - a_2)\cdots(x - a_t)$ divides $f(x)$. Thus degree $f(x) \geq t$. □

Definition 2.3. We say that a is a **root of multiplicity** t for $f(x) \in k[x]$ when $(x - a)^t$ divides $f(x)$ but $(x - a)^{t+1}$ does not.

Let's briefly consider the evaluation at a homomorphism for a fixed $a \in k$.

$$\begin{aligned} \varphi_a : k[x] &\longrightarrow k \\ f(x) &\longmapsto f(a) \end{aligned}$$

The homomorphism is surjective. By the roots-factors theorem, the kernel of this map is the set of polynomials that are multiples of $x-a$. That is, the ideal $\langle x - a \rangle$.

Polynomial Rings in Several Variables

Now we consider $k[x_1, x_2, \ldots, x_n]$. We will default to n being the number of variables, and to be concise I will sometimes write $k[\bar{x}]$.

Definition 2.4. Let $x_1, \ldots, x_n$ be variables (more properly indeterminates, but variables is easier to say). A *monomial* is a product $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ with each α_i a nonnegative integer. We will call $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{N}_0^n$ the **exponent vector** for this monomial and we will use the shorthand x^α for $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$. The **total degree** of x^α is $|\alpha| = \alpha_1 + \cdots + \alpha_n$.

An element of $k[\bar{x}]$ is a sum of **terms**, each term being a constant multiple of a monomial. So, elements of $k[\bar{x}]$ will be written

$$f = \sum_\alpha f_\alpha x^\alpha$$

Here $f_\alpha \in k$ is the **coefficient** of x^α. The sum is implicitly over a *finite* subset of $\mathbb{N}_0^n$. Alternatively, we may consider the sum to be over all of $\mathbb{N}_0^n$, but only a finite number of the f_α are nonzero. This finiteness assumption will be implicit whenever we write a polynomial in this way.

Each $f \in k[\bar{x}]$ determines a function:

$$\begin{aligned} f : k^n &\longrightarrow k \\ \bar{b} &\longmapsto f(\bar{b}) = \sum_{\alpha} f_\alpha b_1^{\alpha_1} b_2^{\alpha_2} \cdots b_n^{\alpha_n} \end{aligned}$$

As with the case $n = 1$ discussed above, we can consider the graph of $f(\bar{x})$ in k^{n+1}. That is, the set of $(\bar{x}, y)$ points $(\bar{x}, f(\bar{x}))$. Slicing it with $y = 0$ we get the "zero-set" of f.

Definition 2.5. The **variety** defined by $f \in k[\bar{x}]$ (also called the zero-set of f) is

$$\mathbb{V}(f) = \left\{\bar{b} \in k^n : f(\bar{b}) = 0\right\}$$

Similarly, for any set of polynomials F

$$\mathbb{V}(F) = \left\{\bar{b} \in k^n : f(\bar{b}) = 0 \text{ for all } f \in F\right\}$$

Discussion: Properties of varieties

A simple logical argument shows the following.

Proposition 2.6. *For $f, g \in k[\bar{x}]$, $\mathbb{V}(f) \cap \mathbb{V}(g) = \mathbb{V}(f, g)$. More generally, for any set F of polynomials.*

$$\mathbb{V}(F) = \bigcap_{f \in F} \mathbb{V}(f)$$

Here is another logical consequence of the definition of a variety.

Proposition 2.7. *If $F \subseteq G$ then $\mathbb{V}(F) \supseteq \mathbb{F}(G)$.*

It is less clear that the union of varieties is a variety, but that is also true.

Proposition 2.8.

$$\mathbb{V}(F) \cup \mathbb{V}(G) = \mathbb{V}(\{fg : f \in F \text{ and } g \in G\})$$

More generally, any finite union of varieties is a variety.

Proof. §1.2 Lemma 2. □

Here is a weird example.

Example 2.9. Let q be a prime power. Consider $x^q - x \in \mathbb{F}_q[x, y]$. Since $\alpha^q = \alpha$ for every element of $\mathbb{F}_q$, the variety of $x^q - x$ is the whole plane over $\mathbb{F}_q$: $\mathbb{V}(x^q - x) = \mathbb{F}_q^2$.

We will generally work over infinite fields, which, as the following proposition shows, allows us to avoid the behaviour in the example.

Proposition 2.10. *For k an infinite field and $f \in k[\bar{x}]$, $\mathbb{V}(f) = 0$ if and only if $f = 0$.*

Consequently, if $f, g \in k[\bar{x}]$ and $f(\bar{a}) = g(\bar{a})$ for all $\bar{a} \in k^n$ then $f = g$.

Proof. §1.1 Prop. 5. and Cor. 6. □

Exercises 2.11.

(a) Varieties in k^1 are finite.

(b) A finite set of points in k^n is a variety.

Exercises 2.12. There are 6 ways to think of $k[x, y, z]$ as a succession of one variable polynomial rings $k[x][y][z]$ or $k[y][x][z]$ etc..

(a) Write the polynomial $x^2y+x^2z+y^3z+yz^3+y^2x+x+y+z$ using descending degree in each of these rings.

(b) Find a polynomial that has as few terms as possible and has a different leading term in each of the different ways to think about $k[x, y, z]$.

Exercises 2.13. From [CLO] Section 1.2.

(a) §1.2 #2 sketch an eliptic curve,

(b) §1.2 #4de sketch,

(c) §1.2 #5 sketch for a product ideal,

(d) §1.2 #13, 14 robot arm problems

(e) (HW) §1.2 #15d The Cartesian product of two varieties is a variety.

A final point on the ground field

Algebraic geometry is usually conducted over an algebraically closed field (at least as a starting point) so that every polynomial in one variable factors completely (into linear factors). We will see that this has an important impact for varieties in higher dimensions as well.

The algebraically closed fields that we will use are $\mathbb{C}$, and $\overline{\mathbb{F}}_p = \bigcup_n \mathbb{F}_{p^n}$ (occassionally), and $\overline{\mathbb{Q}}$ (very rarely).

3 Algebra and Geometry: Ideals and Varieties

Ideals and some special properties of them

Definition 3.1. An **ideal** of a ring R is a nonempty subset $I \subseteq R$ which is closed under addition and closed under multiplication by an arbitrary element of R:

$$a + b \in I \qquad \text{if } a, b \in I \tag{1}$$

$$ra \in I \qquad \text{if } a \in I \text{ and } r \in R \tag{2}$$

We will say that I is an additive subgroup of R and I **absorbs products**. (If $a \in I$ then so is its additive inverse since $(-1)a \in I$, so I is a subgroup under addition.)

There are 3 types of ideals that will play a prominent role in this course.

Definition 3.2. Let I be a proper ideal of R (that is $I \neq R$). An ideal I is **maximal** if the only ideal properly containing I is R. The ideal I is **prime** when $ab \in I$ implies that either $a \in I$ or $b \in I$. The ideal I is **radical** when $a^n \in I$ for $n \in \mathbb{N}$ implies $a \in I$.

Points and maximal ideals

In the last section we focused on the function defined by $f \in k[\bar{x}]$.

$$\begin{aligned} f : k^n &\longrightarrow k \\ \bar{b} &\longmapsto f(\bar{b}) = \sum_{\alpha} f_\alpha b_1^{\alpha_1} b_2^{\alpha_2} \cdots b_n^{\alpha_n} \end{aligned}$$

We now shift attention: for a fixed $\bar{b} \in k^n$ we have a homomorphism

$$\begin{aligned} \varphi_{\bar{b}} : k[\bar{x}] &\longrightarrow k \\ x_i &\longmapsto b_i \\ f(\bar{x}) &\longmapsto f(\bar{b}) = \sum_{\alpha} f_\alpha b_1^{\alpha_1} b_2^{\alpha_2} \cdots b_n^{\alpha_n} \end{aligned}$$

This is a homomorphism by the universal property of polynomial rings.

The kernel of $\varphi_{\bar{b}}$ is the maximal ideal $\langle x_1 - b_1, x_2 - b_2, \ldots, x_n - b_n \rangle$. Consequently, for $f \in k[\bar{x}]$ we have the equivalences

$$\begin{aligned} \bar{b} \in \mathbb{V}(f) &\iff f(\bar{b}) = 0 \\ &\iff \varphi_{\bar{b}}(f) = 0 \\ &\iff f \in \langle x_1 - b_1, x_2 - b_2, \ldots, x_n - b_n \rangle \end{aligned}$$

Thus a geometric statement—$\bar{b}$ is a point of the variety defined by f—has an algebraic analogue—f is in the maximal ideal $\langle x_1 - b_1, x_2 - b_2, \ldots, x_n - b_n \rangle$.

Discussion: Ideal of a set of points

We have defined the variety for any set of polynomials $F \subseteq k[\bar{x}]$ to be the points $\bar{b}$ in k^n such that all $f \in F$ vanish at $\bar{b}$. The first thing we should note is that the variety defined by a set of polynomials is equal to the variety defined by the ideal those polynomials generate.

Proposition 3.3. $\mathbb{V}(F) = \mathbb{V}(\langle F \rangle)$

As an opposite operation to $\mathbb{V}$ (which, given polynomials determines a set of points in k^n) we define an operator that, given a set of points determines a set of polynomials.

Definition 3.4. Let S be a set of points in k^n, the *ideal defined by* S is

$$\mathbb{I}(S) = \left\{ f \in k[\bar{x}] : f(\bar{b}) = 0 \text{ for all } \bar{b} \in S \right\}$$

Proposition 3.5. *$\mathbb{I}(S)$ is not only an ideal, it is a radical ideal.*

Proposition 3.6. *If $S \subseteq T$ then $\mathbb{I}(S) \supseteq \mathbb{I}(T)$.*

Exercises 3.7.

(a) §1.4 #3, 5 Equality of ideals.

Discussion: Composition of $\mathbb{I}$ and $\mathbb{V}$

Proposition 3.8.

$$\mathbb{V}(\mathbb{I}(S)) \supseteq S$$
$$\mathbb{I}(\mathbb{V}(F)) \supseteq F$$

Proposition 3.9.

$$\mathbb{I}\big(\mathbb{V}(\mathbb{I}(S))\big) = \mathbb{I}(S)$$
$$\mathbb{V}\big(\mathbb{I}(\mathbb{V}(F))\big) = \mathbb{V}(F)$$

4 Parametrization and Implicitization

From a practical point of view, how does one describe a set of points in k^n? Listing the points limits us to a finite set. In order to get an infinite set we might use a parametrization. As an example over $\mathbb{R}$, the set of points $(\cos(t), \sin(t))$ in the plane satisfy the polynomial equation $x^2 + y^2 = 1$. Conversely, for any point on $x^2 + y^2 = 1$ there is a choice of t the produces that point. The circle may also be parametrized by $((1-t^2)/(1+t^2), 2t/(1+t^2))$, although this parametrization does not yield the point $(-1, 0)$. This is not a parametrization by polynomial functions, but it is close, we used rational polynomials.

We focus on parametrizations by polynomial or rational polynomial functions. A key question is, how does one determine the ideal of polynomials that vanish on the set S that is the image of the parametrization? This is called **implicitization**. A second question is, are there additional points on the variety defined by the ideal, $\mathbb{V}(\mathbb{I}(S))$?

There is also a natural reverse question. Given an ideal I in $k[\bar{x}]$ can we parametrize the points $\mathbb{V}(I)$? Or, perhaps "most of" them?

[CLO] §1.3 treats several examples. First, they parametrize a variety determined by linear equations. Then the treat the circle, deriving the parametrization above via a geometric argument. They give an implictly defined surface $x^2 - y^2z + z^3$, and a parametrization for it (which is derived in §1.3 problem 11. They then describe another pametrically defined surface: the tangent surface of the twisted cubic curve (the curve defined by the parametrization (t, t^2, t^3)). They give the implicit description of the surface as a teaser for §3.3 where the techniques for implicitization are treated in detail.

It is interesting to note the different utility of parametric vs implicit descriptions. To create a point on a variety the parametric description is useful, and the implicit description is not very useful. On the other hand, to check if a given point $\bar{a}$ is on a variety, the implicit description is useful and the parametric is not.

4.1. Discussion and HW problems

Here are the main problems to do to get a sense for the implicitization and parametrization.

Implicitly and parametrically defined varieties.

(1) (HW)§1.2 #8 the punctured line is not a variety.

(2) §1.3 #4 Implicitization of a parametrized curve.

(3) §1.3 #5(b,c,d) Parametrizing the hyperbola.

(4) (HW) §1.3 #6 Parametrizing the sphere.

(5) §1.3 #11 parametrizing $x^2 - y^2z + z^3$.

(6) (HW) §1.4 #11, 12 The variety of a parametrized curve.

Implicitization and parametrization

(1) II.1 #1d ideal membership in $k[x]$.

(2) II.1#2b Parametrize a variety described by linear equations.

(3) II.1#3b,c Find an implicit description of (the ideal of) a parametrized variety.

(4) (HW) II.1#5a-c Implicit formula for a parametrically defined curve in the plane.

Chapter 2 of [CLO] starts with some big issues and questions concerning the relationship between algebra and geometry. I've added some others. The quoted problems are from [CLO] §2.1.

- We can understand change of coordinates as an isomorphism of polynomial rings.
- What is the "best" way to describe a variety? (The "ideal description" problem.)
- How can we determine if a polynomial is in a particular ideal (or vanishes on a particular variety)? (The "ideal membership" problem.)
- Is there a way to describe the points on a variety explictly? Conic sections can be parametrized, but not all varieties are parametrizable. (The "solving polynomial equations" problem.)
- Parametrization: We can understand it as a homomorphism of rings. Can we find the ideal of a parametrized variety? (The "implicitization" problem.
- Singularities and other special points. We can understand singularities and differentiate types of singularities algebraically.
- Intersection of varieties: We can understand intersections and tangency better by considering algebraic properties.
- Families of curves as slices of surfaces (and ditto for higher dimension). The "special" slices may be understood algebraically.