# Appendix A

# Appendix

## A.1 Algebra

Algebra is the foundation of algebraic geometry; here we collect some of the basic algebra on which we rely. We develop some algebraic background that is needed in the text. This may not be an adequate substitute for a course in abstract algebra. Proofs can be found in give some useful texts.

### A.1.1 Fields and Rings

We are all familiar with the real numbers, $\mathbb{R}$, with the rational numbers $\mathbb{Q}$, and with the complex numbers $\mathbb{C}$. These are the most common examples of *fields*, which are the basic building blocks of both the algebra and the geometry that we study. Formally and briefly, a field is a set $\mathbb{F}$ equipped with operations of addition and multiplication and distinguished elements 0 and 1 (the additive and multiplicative identities). Every number $a \in \mathbb{F}$ has an additive inverse $-a$ and every non-zero number $a \in \mathbb{F}^\times := \mathbb{F} - \{0\}$ has a multiplicative inverse $a^{-1} =: \frac{1}{a}$. Addition and multiplication are commutative and associative and multiplication distributes over addition, $a(b + c) = ab + ac$. To avoid triviality, we require that $0 \neq 1$.

The set of integers $\mathbb{Z}$ is not a field as $\frac{1}{2}$ is not an integer. While we will mostly be working over $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, at times we will need to discuss other fields. Most of what we do in algebraic geometry makes sense over any field, including the finite fields. In particular, linear algebra (except numerical linear algebra) works over any field.

Linear algebra concerns itself with *vector spaces*. A vector space $V$ over a field $\mathbb{F}$ comes equipped with an operation of addition—we may add vectors and an operation of multiplication—we may multiply a vector by an element of the field. A linear combination of vectors $v_1, \ldots, v_n \in V$ is any vector of the form

$$a_1 v_1 + a_2 v_2 + \cdots + a_n v_n \,,$$

where $a_1, \ldots, a_n \in \mathbb{F}$. A collection $S$ of vectors *spans* $V$ if every vector in $V$ is a linear

combination of vectors from $S$. A collection $S$ of vectors is *linearly independent* if zero is not nontrival linear combination of vectors from $S$. A *basis* $S$ of $V$ is a linearly independent spanning set. When a vector space $V$ has a finite basis, every other basis has the same number of elements, and this common number is called the *dimension* of $V$.

A *ring* is the next most complicated object we encounter. A ring $R$ comes equipped with an addition and a multiplication which satisfy almost all the properties of a field, except that we do not necessarily have multiplicative inverses. While the integers $\mathbb{Z}$ do not form a field, they do form a ring. An *ideal* $I$ of a ring $R$ is a subset which is closed under addition and under multiplication by elements of $R$. Every ring has two trivial ideals, the zero ideal $\{0\}$ and the unit ideal consisting of $R$ itself. Given a set $S \subset R$ of elements, the smallest ideal containing $S$, also called the ideal *generated by* $S$, is

$$\langle S \rangle \;:=\; \{r_1 s_1 + r_2 s_2 + \cdots + r_m s_m \mid r_1, \ldots, r_m \in R \text{ and } s_1, \ldots, s_m \in S\}\,.$$

A primary use of ideals in algebra is through the construction of quotient rings. Let $I \subset R$ be an ideal. Formally, the *quotient ring* $R/I$ is the collection of all sets of the form

$$[r] \;:=\; r + I \;=\; \{r + s \mid s \in I\}\,,$$

as $r$ ranges over $R$. Addition and multiplication of these sets are defined in the usual way

$$\begin{aligned} [r] + [s] &= \{r' + s' \mid r' \in [r] \text{ and } s' \in [s]\} \stackrel{!}{=} [r+s], \quad \text{and} \\ [r] \cdot [s] &= \{r' \cdot s' \mid r' \in [r] \text{ and } s' \in [s]\} \stackrel{!}{=} [rs]\,. \end{aligned}$$

The last equality ($\stackrel{!}{=}$) in each line is meant to be surprising, it is a theorem and due to $I$ being an ideal. Thus addition and multiplication on $R/I$ are inherited from $R$. With these definitions (and also $-[r] = [-r]$, $0 := [0]$, and $1 := [1]$), the set $R/I$ becomes a ring.

We say '$R$-mod-$I$' for $R/I$ because the arithmetic in $R/I$ is just the arithmetic in $R$, but considered modulo the ideal $I$, as $[r] = [s]$ in $R/I$ if and only if $r - s \in I$.

Ideals also arise naturally as kernels of homomorphisms. A *homomorphism* $\varphi\colon R \to S$ from the ring $R$ to the ring $S$ is a function that preserves the ring structure. Thus for $r, s \in R$, $\varphi(r+s) = \varphi(r) + \varphi(s)$ and $\varphi(rs) = \varphi(r)\varphi(s)$. We also require that $\varphi(1) = 1$. The *kernel* of a homomorphism $\varphi\colon R \to S$,

$$\ker \varphi \;:=\; \{r \in R \mid \varphi(r) = 0\}$$

is an ideal: If $r, s \in \ker\varphi$ and $t \in R$, then

$$\varphi(r+s) \;=\; \varphi(r) + \varphi(s) \;=\; 0 \;=\; t\varphi(r) \;=\; \varphi(tr)\,.$$

Homomorphisms are deeply intertwined with ideals. If $I$ is an ideal of a ring $R$, then the association $r \mapsto [r]$ defines a homomorphism $\varphi\colon R \to R/I$ whose kernel is $I$. Dually, given a homomorphism $\varphi\colon R \to S$, the image of $R$ in $S$ is identified with $R/\ker\varphi$. More

generally, if $\varphi\colon R \to S$ is a homomorphism and $I \subset R$ is an ideal with $I \subset \ker \varphi$ (that is, $\varphi(I) = 0$), then $\varphi$ induces a homomorphism $\varphi\colon R/I \to S$.

Properties of ideals induce natural properties in the associated quotient rings. An element $r$ of a ring $R$ is *nilpotent* if $r \neq 0$, but some power of $r$ vanishes. A ring $R$ is *reduced* if it has no nilpotent elements, that is, whenever $r \in R$ and $n$ is a natural number with $r^n = 0$, then we must have $r = 0$. An ideal *radical* if whenever $r \in R$ and $n$ is a natural number with $r^n \in I$, then we must have $r \in I$. It follows that a quotient ring $R/I$ is reduced if and only if $I$ is radical.

A ring $R$ is a *domain* if whenever we have $r \cdot s = 0$ with $r \neq 0$, then we must have $s = 0$. An ideal is *prime* if whenever $r \cdot s \in I$ with $r \notin I$, then we must have $s \in I$. It follows that a quotient ring $R/I$ is a domain if and only if $I$ is prime.

A ring $R$ with no nontrivial ideals must be a field. Indeed, if $0 \neq r \in R$, then the ideal $rR$ of $R$ generated by $r$ is not the zero ideal, and so it must equal $R$. But then $1 = rs$ for some $s \in R$, and so $r$ is invertible. Conversely, if $R$ is a field and $0 \neq r \in R$, then $1 = r \cdot r^{-1} \in rR$, so the only ideals of $R$ are $\{0\}$ and $R$. An ideal $\mathfrak{m}$ of $R$ is *maximal* if $\mathfrak{m} \subsetneq R$, but there is no ideal $I$ strictly contained between $\mathfrak{m}$ and $R$; if $\mathfrak{m} \subset I \subset R$ and $I \neq R$, then $I = \mathfrak{m}$. It follows that a quotient ring $R/I$ is a field if and only if $I$ is maximal.

Lastly, we remark that any ideal $I$ of $R$ with $I \neq R$ is contained in some maximal ideal. Suppose not. Then we may find an infinite chain of ideals

$$I \;=:\; I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots$$

where each is proper so that 1 lies in none of them. Set $J := \bigcup_n I_n$. Then we claim that the union $I := \bigcup_n I_n$ of these ideals is an ideal. Indeed, if $r, s \in I$ then there are indices $i, j$ with $r \in I_i$ and $s \in I_j$. Since $I_i, I_j \subset I_{\max(i,j)}$, we have $r + s \in I_{\max(i,j)} \subset J$. If $t \in R$, then $tr \in I_i \subset J$

## A.1.2 Fields and polynomials

Our basic algebraic objects are polynomials. A *univariate polynomial* $p$ is an expression of the form

$$p \;=\; p(x) \;:=\; a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m\,, \tag{A.1}$$

where $m$ is a nonnegative integer and the coefficients $a_0, a_1, \ldots, a_m$ lie in $\mathbb{F}$. Write $\mathbb{F}[x]$ for the set of all polynomials in the variable $x$ with coefficients in $\mathbb{F}$. We may add, subtract, and multiply polynomials and $\mathbb{F}[x]$ is a ring.

While a polynomial $p$ may be regarded as a formal expression (A.1), evaluation of a polynomial defines a function $p\colon \mathbb{F} \to \mathbb{F}$: The value of the function $p$ at a point $a \in \mathbb{F}$ is simply $p(a)$. When $\mathbb{F}$ is infinite, the polynomial and the function determine each other, but this is not the case when $\mathbb{F}$ is finite.

Our study requires polynomials with more than one variable. We first define a monomial.

**Definition.** A *monomial* in the variables $x_1, \ldots, x_n$ is a product of the form

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} ,$$

where the exponents $\alpha_1, \ldots, \alpha_n$ are nonnegative integers. For notational convenience, set $\alpha := (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ and write $x^\alpha$ for the expression $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. The *(total) degree* of the monomial $x^\alpha$ is $|\alpha| := \alpha_1 + \cdots + \alpha_n$.

A *polynomial* $f = f(x_1, \ldots, x_n)$ in the variables $x_1, \ldots, x_n$ is a linear combination of monomials, that is, a finite sum of the form

$$f \;=\; \sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha ,$$

where each *coefficient* $a_\alpha$ lies in $\mathbb{F}$ and all but finitely many of the coefficients vanish. The product $a_\alpha x^\alpha$ of an element $a_\alpha$ of $\mathbb{F}$ and a monomial $x^\alpha$ is called a *term*. The *support* $\mathcal{A} \subset \mathbb{N}^n$ of a polynomial $f$ is the set of all exponent vectors that appear in $f$ with a nonzero coefficient. We will say that $f$ has support $\mathcal{A}$ when we mean that the suport of $f$ is a subset of $\mathcal{A}$.

After 0 and 1 (the additive and multiplicative identities), the most distinguished integers are the prime numbers, those $p > 1$ whose only divisors are 1 and themselves. These are the numbers $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$ Every integer $n > 1$ has a unique factorization into prime numbers

$$n \;=\; p_1^{\alpha_1} p_1^{\alpha_2} \cdots p_n^{\alpha_n} ,$$

where $p_1 < \cdots < p_n$ are distinct primes, and $\alpha_1, \ldots, \alpha_n$ are (strictly) positive integers. For example, $999 = 3^3 \cdot 37$. Polynomials also have unique factorization.

**Definition.** A nonconstant polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ is *irreducible* if whenever we have $f = gh$ with $g, h$ polynomials, then either $g$ or $h$ is a constant. That is, $f$ has no nontrivial factors.

**Theorem A.1.1** *Every polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ is a product of ireducible polynomials*

$$f \;=\; p_1 \cdot p_2 \cdots p_m ,$$

*where the polynomials $p_1, \ldots, p_m$ are irreducible and nonconstant. Moreover, this factorization is essentially unique. That is, if*

$$f \;=\; q_1 \cdot q_2 \cdots q_s ,$$

*is another such factorization, then $m = s$, and after permuting the order of the factors, each polynomial $q_i$ is a scalar multiple of the corresponding polynomial $p_i$.*

### A.1.3 Polynomials in one variable

While rings of polynomials have many properties in common with the integers, the relation is the closest for univariate polynomials. The *degree*, $\deg(f)$ of a univariate polynomial $f$ is the largest degree of a monomial appearing in $f$. If this monomial has coefficent 1, then the polynomial is *monic*. This allows us to remove the ambiguity in the uniqueness of factorizations in Theorem A.1.1. A polynomial $f(x) \in \mathbb{F}[x]$ has a unique factorization of the form

$$f \;=\; f_m \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_s^{\alpha_s}\,,$$

where $f_m \in \mathbb{F}^\times$ is the leading coefficient of $f$, the polynomials $p_1, \ldots, p_s$ are monic and irreducible, and the exponents $\alpha_i$ are positive integers.

**Definition.** A *greatest common divisor* of two polynomials $f, g \in \mathbb{F}[x]$ (or $\gcd(f,g)$) is a polynomial $h$ such that $h$ divides each of $f$ and $g$, and if there is another polynomial $k$ which divides both $f$ and $g$, then $k$ divides $h$.

Any two polynomials $f$ and $g$ have a monic greatest common divisor which is the product of the common monic irreducible factors of $f$ and $g$, each raised to the highest power that divdes both $f$ and $g$. Finding greatest comon divisor would seem challenging as factoring polynomials is not an easy task. There is, however, a very fast and efficient algorithm for computing the greatest common divisor of two polynomials.

Suppose that we have polynomials $f$ and $g$ in $\mathbb{F}[x]$ with $\deg(g) \geq \deg(f)$,

$$\begin{aligned} f &= f_0 + f_1 x + f_2 x^2 + \cdots + f_m x^m \\ g &= g_0 + g_1 x + g_2 x^2 + \cdots + g_m x^m + \cdots + g_n x^n\,, \end{aligned}$$

where $f_m$ and $g_n$ are nonzero. Then the polynomial

$$S(f,g) \;:=\; g - \frac{g_n}{f_m} x^{n-m} \cdot f$$

has degree strictly less than $n = \deg(g)$. This simple operation of *reducing* $f$ by the polynomial $g$ forms the basis of the Division Algorithm and the Euclidean Algorithm for computing the greatest common divisor of two polynomials.

We describe the *Division Algorithm* in *pseudocode*, which is a common way to explain algorithms without reference to a specific programming language.

**Division Algorithm.**
INPUT: Polynomials $f, g \in \mathbb{F}[x]$.
OUTPUT: Polynomials $q, r \in \mathbb{F}[x]$ with $g = qf + r$ and $\deg(r) < \deg(f)$.
Set $r := g$ and $q := 0$.
(1) If $\deg(r) < \deg(f)$, then exit.
(2) Otherwise, reduce $r$ by $f$ to get the expression

$$r \;=\; \frac{r_n}{f_m} x^{n-m} \cdot f \;+\; S(f,r)\,,$$

where $n = \deg(r)$ and $m = \deg(f)$. Set $q := q + \frac{r_n}{f_m} x^{n-m}$ and $r := r - S(f, r)$, and return to step (1).

To see that this algorithm does produce the desired expression $g = qf + r$ with the degree of $r$ less than the degree of $f$, note first that whenever we are at step (1), we will always have $g = qf + r$. Also, every time step (2) is executed, the degree of $r$ must drop, and so after at most $\deg(g) - \deg(f) + 1$ steps, the algorithm will halt with the correct answer.

The *Euclidean Algorithm* computes the greatest common divisor of two polynomials $f$ and $g$.

**Euclidean Algorithm.**
INPUT: Polynomials $f, g \in \mathbb{F}[x]$.
OUTPUT: The greatest common divisor $h$ of $f$ and $g$.
(1) Call the Division Algorithm to write $g = qf + r$ where $\deg(r) < \deg(f)$.
(2) If $r = 0$ then set $h := f$ and exit.
Otherwise, set $g := f$ and $f := r$ and return to step (1).

To see that the Euclidean algorithm performs as claimed, first note that if $g = qf + r$ with $r = 0$, then $f = \gcd(f, g)$. If $r \neq 0$, then $\gcd(f, g) = \gcd(f, r)$. Thus the greatest common divisor $h$ of $f$ and $g$ is always the same whenever step (1) is executed. Since the degree of $r$ must drop upon each iteration, $r$ will eventually become 0, which shows that the algorithm will halt and return $h$.[†]

An ideal is *principal* if it has the form

$$\langle f \rangle \;=\; \{h \cdot f \mid h \in \mathbb{F}[x]\}\,,$$

for some $f \in \mathbb{F}[x]$. We say that $f$ *generates* $\langle f \rangle$. Since $\langle f \rangle = \langle \alpha f \rangle$ for any $\alpha \in \mathbb{F}$, the principal ideal has a unique monic generator.

**Theorem A.1.2** *Every ideal $I$ of $\mathbb{F}[x]$ is principal.*

*Proof.* Suppose that $I$ is a nonzero ideal of $\mathbb{F}[x]$, and let $f$ be a nonzero polynomial of minimal degree in $I$. If $g \in I$, then we may apply the Division Algorithm and obtain polynomials $q, r \in \mathbb{F}[x]$ with

$$g \;=\; qf + r \qquad \text{with} \qquad \deg(r) < \deg(f)\,.$$

Since $r = g - qf$, we have $r \in I$, and since $\deg(r) < \deg(f)$, but $f$ had minimal degree in $I$, we conclude that $f$ divides $g$, and thus $I = \langle f \rangle$. □

[†]This is poorly written!

The ideal generated by univariate polynomials $f_1, \ldots, f_s$ is the principal ideal $\langle p \rangle$, where $p$ is the greatest common divisor of $f_1, \ldots, f_s$.

For univariate polynomials $p$ the quotient ring $\mathbb{F}[x]/\langle p \rangle$ has a concrete interpretation. Given $f \in \mathbb{F}[x]$, we may call the Division Algorithm to obtain polynomials $q, r$ with

$$f \;=\; q \cdot p + r, \text{ where } \deg(r) < \deg(q)\,.$$

Then $[f] = f + \langle p \rangle = r + \langle p \rangle = [r]$ and in fact $r$ is the unique polynomial of minimal degree in the coset $f + \langle p \rangle$. We call this the *normal form* of $f$ in $\mathbb{F}[x]/\langle p \rangle$.

Since, if $\deg(r), \deg(s) < \deg(p)$, we cannot have $r - s \in \langle p \rangle$ unless $r = s$, we see that the monomials $1, x, x^2, \ldots, x^{\deg(p)-1}$ form a basis for the $\mathbb{F}$-vector space $\mathbb{F}[x]/\langle p \rangle$. This describes the aditive structure on $\mathbb{F}[x]/\langle p \rangle$.

To describe its multiplicative structure, we only need to show how to write a product of monomials $x^a \cdot x^b$ with $a, b < \deg(p)$ in this basis. Suppose that $p$ is monic with $\deg(p) = n$ and write $p(x) = x^n - q(x)$, where $q$ has degree strictly less than $p$. Since $x^a \cdot x^b = (x^a \cdot x) \cdot x^{b-1}$, we may assume that $b = 1$. When $a < n$, we have $x^a \cdot x^1 = x^{a+1}$. When $a = n - 1$, then $x^{n-1} \cdot x^1 = x^n = q(x)$,

- Relate algebraic properties of $p(x)$ to properties of $R$, for example, zero divisors and domain.
- Prove that a field is a ring with only trivial ideals.

  Prove $I \subset J \subset R$ are ideals, then $J/I$ is an ideal of $R/I$, and dedice that $R = \mathbb{F}[x]/p(x)$ is a field only if $p(x)$ is irreducible.

  Example $\mathbb{Q}[x]/(x^2 - 2)$ and explore $\mathbb{Q}(\sqrt{2})$.

  Example $\mathbb{R}[x]/(x^2 + 1)$ and show how it is isomorphic to $\mathbb{C}$.

  Work up to algebraically closed fields, the fundamental theoerem of algebra (both over $\mathbb{C}$ and over $\mathbb{R}$).

  Explain that an algebraically closed field has no algebraic extensions (hence the name).
- Define the maximal ideal $\mathfrak{m}_a$ for $a \in \mathbb{A}^n$.

  **Theorem A.1.3** *The maximal ideals of* $\mathbb{C}[x_1, \ldots, x_n]$ *all have the form* $\mathfrak{m}_a$ *for some* $a \in \mathbb{A}^n$.

## A.2 Topology

Collect some topological statements here. Definition of topology, Closed/open duality, dense, nowhere dense... Describe the usual topology.