Appendix A

Some Concepts from Algebra

This appendix contains precise statements of various algebraic facts and definitions used in the text. For students who have had a course in abstract algebra, much of this material will be familiar. For students seeing these terms for the first time, keep in mind that the abstract concepts defined here are used in the text in very concrete situations.

§1 Fields and Rings

We first give a precise definition of a field.

Definition 1. *A* **field** *consists of a set k and two binary operations "$\cdot$" and "$+$" defined on k for which the following conditions are satisfied:*

(i) $(a + b) + c = a + (b + c)$ *and* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *for all* $a, b, c \in k$ *(associative).*
(ii) $a + b = b + a$ *and* $a \cdot b = b \cdot a$ *for all* $a, b \in k$ *(commutative).*
(iii) $a \cdot (b + c) = a \cdot b + a \cdot c$ *for all* $a, b, c \in k$ *(distributive).*
(iv) *There are* $0, 1 \in k$ *such that* $a + 0 = a \cdot 1 = a$ *for all* $a \in k$ *(identities).*
(v) *Given* $a \in k$, *there is* $b \in k$ *such that* $a + b = 0$ *(additive inverses).*
(vi) *Given* $a \in k, a \neq 0$, *there is* $c \in k$ *such that* $a \cdot c = 1$ *(multiplicative inverses).*

The fields most commonly used in the text are $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. In the exercises to §1 of Chapter 1, we mention the field $\mathbb{F}_2$ which consists of the two elements 0 and 1. Some more complicated fields are discussed in the text. For example, in §3 of Chapter 1, we define the field $k(t_1, \ldots, t_m)$ of rational functions in $t_1, \ldots, t_m$ with coefficients in k. Also, in §5 of Chapter 5, we introduce the field $k(V)$ of rational functions on an irreducible variety V.

If we do not require multiplicative inverses, then we get a commutative ring.

Definition 2. *A* **commutative ring** *consists of a set R and two binary operations "$\cdot$" and "$+$" defined on R for which the following conditions are satisfied:*

(i) $(a + b) + c = a + (b + c)$ *and* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *for all* $a, b, c, \in R$ *(associative).*

(ii) $a + b = b + a$ *and* $a \cdot b = b \cdot a$ *for all* $a, b \in R$ *(commutative).*
(iii) $a \cdot (b + c) = a \cdot b + a \cdot c$ *for all* $a, b, c \in R$ *(distributive).*
(iv) *There are* $0, 1 \in R$ *such that* $a + 0 = a \cdot 1 = a$ *for all* $a \in R$ *(identities).*
(v) *Given* $a \in R$, *there is* $b \in R$ *such that* $a + b = 0$ *(additive inverses).*

Note that any field is obviously a commutative ring. Other examples of commutative rings are the integers $\mathbb{Z}$ and the polynomial ring $k[x_1, \ldots, x_n]$. The latter is the most commonly used ring in the book. In Chapter 5, we construct two other commutative rings: the coordinate ring $k[V]$ of polynomial functions on an affine variety V and the quotient ring $k[x_1, \ldots, x_n]/I$, where I is an ideal of $k[x_1, \ldots, x_n]$.

A special case of commutative rings are the *integral domains.*

Definition 3. *A commutative ring* R *is an* **integral domain** *if whenever* $a, b \in R$ *and* $a \cdot b = 0$, *then either* $a = 0$ *or* $b = 0$.

Any field is an integral domain, and the polynomial ring $k[x_1, \ldots, x_n]$ is an integral domain. In Chapter 5, we prove that the coordinate ring $k[V]$ of a variety V is an integral domain if and only if V is irreducible.

Finally, we note that the concept of ideal can be defined for any ring.

Definition 4. *Let* R *be a commutative ring. A subset* $I \subset R$ *is an* **ideal** *if it satisfies:*
(i) $0 \in I$.
(ii) *If* $a, b \in I$, *then* $a + b \in I$.
(iii) *If* $a \in I$ *and* $b \in R$, *then* $b \cdot a \in I$.

Note how this generalizes the definition of ideal given in §4 of Chapter 1.

§2 Groups

A group can be defined as follows.

Definition 1. *A* **group** *consists of a set* G *and a binary operation "*$\cdot$*" defined on* G *for which the following conditions are satisfied:*
(i) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *for all* $a, b, c \in G$ *(associative).*
(ii) *There is* $1 \in G$ *such that* $1 \cdot a = a \cdot 1 = a$ *for all* $a \in G$ *(identity).*
(iii) *Given* $a \in G$, *there is* $b \in G$ *such that* $a \cdot b = b \cdot a = 1$ *(inverses).*

A simple example of a group is given by the integers $\mathbb{Z}$ under addition. Note $\mathbb{Z}$ is not a group under multiplication. A more interesting example comes from linear algebra. Let k be a field and define

$$\mathrm{GL}(n, k) = \{A : A \text{ is an invertible } n \times n \text{ matrix with entries in } k\}.$$

From linear algebra, we know that the product AB of two invertible matrices A and B is again invertible. Thus, matrix multiplication defines a binary operation on $\mathrm{GL}(n, k)$, and it is easy to verify that all of the group axioms are satisfied.

For a final example of a group, let n be a positive integer and consider the set

$$S_n = \{\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\} : \sigma \text{ is one-to-one and onto}\}.$$

Then composition of functions turns S_n into a group. Since elements $\sigma \in S_n$ can be regarded as permutations of the numbers 1 through n, we call S_n the *permutation group*. Note that S_n has $n!$ elements.

Finally, we need the notion of a subgroup.

Definition 2. *Let G be a group. A subset $H \subset G$ is called a* **subgroup** *if it satisfies:*
(i) $1 \in H$.
(ii) *If* $a, b \in H$, *then* $a \cdot b \in H$.
(iii) *If* $a \in H$, *then* $a^{-1} \in H$.

In Chapter 7, we study finite subgroups of the group $\mathrm{GL}(n, k)$.

§3 Determinants

Our first goal is to give a formula for the determinant of an $n \times n$ matrix. We begin by defining the *sign* of a permutation. Recall that the group S_n was defined in §2 of this appendix.

Definition 1. *If $\sigma \in S_n$, let P_σ be the matrix obtained by permuting the columns of the $n \times n$ identity according to σ. Then the* **sign** *of σ, denoted* $\mathrm{sgn}(\sigma)$, *is defined by*

$$\mathrm{sgn}(\sigma) = \det(P_\sigma).$$

Note that we can transform P_σ back to the identity matrix by successively switching columns two at a time. Since switching two columns of a determinant changes its sign, it follows that $\mathrm{sgn}(\sigma)$ equals ± 1. Then one can prove that the determinant is given by the following formula.

Proposition 2. *If $A = (a_{ij})$ is an $n \times n$ matrix, then*

$$\det(A) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}.$$

Proof. A proof is given in Chapter 5, §3 of FINKBEINER (1978). □

This formula is used in a crucial way in our treatment of resultants (see Proposition 8 from Chapter 3, §5).

A second fact we need concerns the solution of a linear system of n equations in n unknowns. In matrix form, the system is written

$$AX = B,$$

where $A = (a_{ij})$ is the $n \times n$ coefficient matrix, B is a column vector, and X is the column vector whose entries are the unknowns $x_1, \ldots, x_n$. When A is invertible, the system has the unique solution given by $X = A^{-1}B$. One can show that this leads to the following explicit formula for the solution.

Proposition 3 (Cramer's Rule). *Suppose we have a system of equations $AX = B$. If A is invertible, then the unique solution is given by*

$$x_i = \frac{\det(M_i)}{\det(A)},$$

where M_i is the matrix obtained from A by replacing its i-th column with B.

Proof. A proof can be found in Chapter 5, §3 of FINKBEINER (1978). □

This proposition is used to prove some basic properties of resultants (see Proposition 9 from Chapter 3, §5).