45. *(n-colorings of graphs)* A finite *graph* $\mathcal{G}$ of size N is a set of vertices $i \in \{1, 2, \ldots, N\}$ and a collection of edges (i, j) connecting vertex i with vertex j. An *n-coloring* of $\mathcal{G}$ is an assignment of one of n colors to each vertex in such a way that vertices connected by an edge have distinct colors. Let F be any field containing at least n elements. If we introduce a variable x_i for each vertex i and represent the n colors by choosing a set S of n distinct elements from F, then an n-coloring of $\mathcal{G}$ is equivalent to assigning a value $x_i = \alpha_i$ for each $i = 1, 2, \ldots, N$ where $\alpha_i \in S$ and $\alpha_i \neq \alpha_j$ if (i, j) is an edge in $\mathcal{G}$. If $f(x) = \prod_{\alpha \in S}(x - \alpha)$ is the polynomial in $F[x]$ of degree n whose roots are the elements in S, then $x_i = \alpha_i$ for some $\alpha_i \in S$ is equivalent to the statement that x_i is a solution to the equation $f(x_i) = 0$. The statement $\alpha_i \neq \alpha_j$ is then the statement that $f(x_i) = f(x_j)$ but $x_i \neq x_j$, so x_i and x_j satisfy the equation $g(x_i, x_j) = 0$, where $g(x_i, x_j)$ is the polynomial $(f(x_i) - f(x_j))/(x_i - x_j)$ in $F[x_i, x_j]$. It follows that finding an *n-coloring* of $\mathcal{G}$ is equivalent to solving the system of equations

$$\begin{cases} f(x_i) = 0, & \text{for } i = 1, 2, \ldots, N. \\ g(x_i, x_j) = 0, & \text{for all edges } (i, j) \text{ in } \mathcal{G} \end{cases}$$

(note also we may use any polynomial g satisfying $\alpha_i \neq \alpha_j$ if $g(\alpha_i, \alpha_j) = 0$). It follows by "Hilbert's Nullstellensatz" (cf. Corollary 33 in Section 15.3) that this system of equations has a solution, hence $\mathcal{G}$ has an n-coloring, unless the ideal I in $F[x_1, x_2, \ldots, x_N]$ generated by the polynomials $f(x_i)$ for $i = 1, 2, \ldots, N$, together with the polynomials $g(x_i, x_j)$ for all the edges (i, j) in the graph $\mathcal{G}$, is not a proper ideal. This in turn is equivalent to the statement that the reduced Gröbner basis for I (with respect to any monomial ordering) is simply $\{1\}$. Further, when an n-coloring does exist, solving this system of equations as in the examples following Proposition 29 provides an explicit coloring for $\mathcal{G}$.

There are many possible choices of field F and set S. For example, use any field F containing a set S of distinct n^{th} roots of unity, in which case $f(x) = x^n - 1$ and we may take $g(x_i, x_j) = (x_i^n - x_j^n)/(x_i - x_j) = x_i^{n-1} + x_i^{n-2}x_j + \cdots + x_i x_j^{n-2} + x_j^{n-1}$, or use any subset S of $F = \mathbb{F}_p$ with a prime $p \geq n$ (in the special case $n = p$, then, by Fermat's Little Theorem, we have $f(x) = x^p - x$ and $g(x_i, x_j) = (x_i - x_j)^{p-1} - 1$).

(a) Consider a possible 3-coloring of the graph $\mathcal{G}$ with eight vertices and 14 edges $(1, 3)$, $(1, 4)$, $(1, 5)$, $(2, 4)$, $(2, 7)$, $(2, 8)$, $(3, 4)$, $(3, 6)$, $(3, 8)$, $(4, 5)$, $(5, 6)$, $(6, 7)$, $(6, 8)$, $(7, 8)$. Take $F = \mathbb{F}_3$ with 'colors' $0, 1, 2 \in \mathbb{F}_3$ and suppose vertex 1 is colored by 0. In this case $f(x) = x(x - 1)(x - 2) = x^3 - x \in \mathbb{F}_3[x]$ and $g(x_i, x_j) = x_i^2 + x_i x_j + x_j^2 - 1$. If I is the ideal generated by $x_1, x_i^3 - x_i$, $2 \leq i \leq 8$ and $g(x_i, x_j)$ for the edges (i, j) in $\mathcal{G}$, show that the reduced Gröbner basis for I with respect to the lexicographic monomial ordering $x_1 > x_2 > \cdots > x_8$ is $\{x_1, x_2, x_3 + x_8, x_4 + 2x_8, x_5 + x_8, x_6, x_7 + x_8, x_8^2 + 2\}$. Deduce that $\mathcal{G}$ has two distinct 3-colorings, determined by the coloring of vertex 8 (which must be colored by a nonzero element in $\mathbb{F}_3$), and exhibit the colorings of $\mathcal{G}$.

Show that if the edge $(3, 7)$ is added to $\mathcal{G}$ then the graph cannot be 3-colored.

(b) Take $F = \mathbb{F}_5$ with four 'colors' $1, 2, 3, 4 \in \mathbb{F}_5$, so $f(x) = x^4 - 1$ and we may use $g(x_i, x_j) = x_i^3 + x_i^2 x_j + x_i x_j^2 + x_j^3$. Show that the graph $\mathcal{G}$ with five vertices having 9 edges $(1, 3)$, $(1, 4)$, $(1, 5)$, $(2, 3)$, $(2, 4)$, $(2, 5)$, $(3, 4)$, $(3, 5)$, $(4, 5)$ (the "complete graph on five vertices" with one edge removed) can be 4-colored but cannot be 3-colored.

(c) Use Gröbner bases to show that the graph $\mathcal{G}$ with nine vertices and 22 edges $(1, 4)$, $(1, 6)$, $(1, 7)$, $(1, 8)$, $(2, 3)$, $(2, 4)$, $(2, 6)$, $(2, 7)$, $(3, 5)$, $(3, 7)$, $(3, 9)$, $(4, 5)$, $(4, 6)$, $(4, 7)$, $(4, 9)$, $(5, 6)$, $(5, 7)$, $(5, 8)$, $(5, 9)$, $(6, 7)$, $(6, 9)$, $(7, 8)$ has precisely four 4-colorings up to a permutation of the colors (so a total of 96 total 4-colorings). Show that if the edge $(1, 5)$ is added then $\mathcal{G}$ cannot be 4-colored.

Part III

MODULES AND VECTOR SPACES

In Part III we study the mathematical objects called modules. The use of modules was pioneered by one of the most prominent mathematicians of the first part of this century, Emmy Noether, who led the way in demonstrating the power and elegance of this structure. We shall see that vector spaces are just special types of modules which arise when the underlying ring is a field. If R is a ring, the definition of an R-module M is closely analogous to the definition of a group action where R plays the role of the group and M the role of the set. The additional axioms for a module require that M itself have more structure (namely that M be an abelian group). Modules are the "representation objects" for rings, i.e., they are, by definition, algebraic objects on which rings act. As the theory develops it will become apparent how the structure of the ring R (in particular, the structure and wealth of its ideals) is reflected by the structure of its modules and vice versa in the same way that the structure of the collection of normal subgroups of a group was reflected by its permutation representations.

CHAPTER 10

Introduction to Module Theory

10.1 BASIC DEFINITIONS AND EXAMPLES

We start with the definition of a module.

Definition. Let R be a ring (not necessarily commutative nor with 1). A *left R-module* or a *left module over R* is a set M together with

(1) a binary operation $+$ on M under which M is an abelian group, and

(2) an action of R on M (that is, a map $R \times M \to M$) denoted by rm, for all $r \in R$ and for all $m \in M$ which satisfies

(a) $(r+s)m = rm + sm$, for all $r, s \in R, m \in M$,

(b) $(rs)m = r(sm)$, for all $r, s \in R, m \in M$, and

(c) $r(m+n) = rm + rn$, for all $r \in R, m, n \in M$.

If the ring R has a 1 we impose the additional axiom:

(d) $1m = m$, for all $m \in M$.

The descriptor "left" in the above definition indicates that the ring elements appear on the left; "right" R-modules can be defined analogously. If the ring R is *commutative* and M is a left R-module we can make M into a right R-module by defining $mr = rm$ for $m \in M$ and $r \in R$. If R is not commutative, axiom 2(b) in general will not hold with this definition (so not every left R-module is also a right R-module). Unless explicitly mentioned otherwise the term "module" will always mean "left module." Modules satisfying axiom 2(d) are called *unital* modules and in this book all our modules will be unital (this is to avoid "pathologies" such as having $rm = 0$ for all $r \in R$ and $m \in M$).

When R is a field F the axioms for an R-module are precisely the same as those for a vector space over F, so that

modules over a field F and vector spaces over F are the same.

Before giving other examples of R-modules we record the obvious definition of submodules.

Definition. Let R be a ring and let M be an R-module. An *R-submodule* of M is a subgroup N of M which is closed under the action of ring elements, i.e., $rn \in N$, for all $r \in R, n \in N$.

Submodules of M are therefore just subsets of M which are themselves modules under the restricted operations. In particular, if $R = F$ is a field, submodules are the same as subspaces. Every R-module M has the two submodules M and 0 (the latter is called the *trivial submodule*).

Examples

(1) Let R be any ring. Then $M = R$ is a left R-module, where the action of a ring element on a module element is just the usual multiplication in the ring R (similarly, R is a right module over itself). In particular, every field can be considered as a (1-dimensional) vector space over itself. When R is considered as a left module over itself in this fashion, the submodules of R are precisely the left ideals of R (and if R is considered as a right R-module over itself, its submodules are the right ideals). Thus if R is not commutative it has a left and right module structure over itself and these structures may be different (e.g., the submodules may be different) — Exercise 21 at the end of this section gives a specific example of this.

(2) Let $R = F$ be a field. As noted above, every vector space over F is an F-module and vice versa. Let $n \in \mathbb{Z}^+$ and let

$$F^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in F, \text{ for all } i\}$$

(called *affine n-space over F*). Make F^n into a vector space by defining addition and scalar multiplication componentwise:

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$
$$\alpha(a_1, \ldots, a_n) = (\alpha a_1, \ldots, \alpha a_n), \qquad \alpha \in F.$$

As in the case of Euclidean n-space (i.e., when $F = \mathbb{R}$), affine n-space is a vector space of dimension n over F (we shall discuss the notion of dimension more thoroughly in the next chapter).

(3) Let R be a ring with 1 and let $n \in \mathbb{Z}^+$. Following Example 2 define

$$R^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in R, \text{ for all } i\}.$$

Make R^n into an R-module by componentwise addition and multiplication by elements of R in the same manner as when R was a field. The module R^n is called *the free module of rank n over R*. (We shall see shortly that free modules have the same "universal property" in the context of R-modules that free groups were seen to have in Section 6.3. We shall also soon discuss direct products of R-modules.) An obvious submodule of R^n is given by the i^{th} component, namely the set of n-tuples with arbitrary ring elements in the i^{th} component and zeros in the j^{th} component for all $j \neq i$.

(4) The same abelian group may have the structure of an R-module for a number of different rings R and each of these module structures may carry useful information. Specifically, if M is an R-module and S is a subring of R with $1_S = 1_R$, then M is automatically an S-module as well. For instance the field $\mathbb{R}$ is an $\mathbb{R}$-module, a $\mathbb{Q}$-module and a $\mathbb{Z}$-module.

(5) If M is an R-module and for some (2-sided) ideal I of R, $am = 0$, for all $a \in I$ and all $m \in M$, we say M is *annihilated by I*. In this situation we can make M into an (R/I)-module by defining an action of the quotient ring R/I on M as follows: for each $m \in M$ and coset $r + I$ in R/I let

$$(r + I)m = rm.$$