Dummit and Foote - Abstract Algebra
Answers to Selected Exercises

Marc-André Brochu

Winter 2019

Chapter 9

Polynomial Rings

9.1 Polynomial Rings over Fields II

For the remaining exercises let F be a field, let F^n be the set of all n-tuples of elements of F (called *affine n-space over F*) and let R be the polynomial ring $F[x_1, x_2, \dots, x_n]$. The elements of R form a ring of F-valued functions on F^n, where the value of the polynomial $p(x_1, \dots, x_n)$ on the n-tuple $(a_1, \dots, a_n)$ is obtained by substituting a_i for x_i for all i.

12.

1. Let X be any given subset of F^n. We always have $0_R \in I(X)$ and thus $I(X)$ is never empty. Take any $f, g \in I(X)$. Then for all $a \in X$, $(f+g)(x) = f(x) + g(x) = 0$. Thus $I(X)$ is closed under addition. Take some $h \in R$. For all $a \in X$, $(h \cdot f)(x) = h(x)f(x) = 0$ which means that $I(X)$ absorbs left multiplication. Because R is commutative, we get that $I(X)$ is an ideal in this ring.

   Let $J \subseteq R$ be arbitrarily given. If $a \in V(\langle J \rangle)$, then for all $f \in J \subseteq \langle J \rangle$, we have that $f(a) = 0$. Thus $V(\langle J \rangle) \subseteq V(J)$. Now let $a \in V(J)$. Take any $f \in \langle J \rangle$. Then f is a finite combination of R-multiples of elements of J, i.e. $f = f_1 j_1 + \dots + f_n j_n$ with $f_i \in R$, $j_i \in J$ and $n \in \mathbb{N}$. So $f(a) = f_1(a)j_1(a) + \dots + f_n(a)j_n(a)$. Since for all $j \in J$, $j(a) = 0$, we get that $f(a) = 0$ and thus $a \in V(\langle J \rangle)$. Therefore $V(J) = V(\langle J \rangle)$ for any subset J of R.

2. Let $f \in I(Y)$. Then for all $a \in X$, a is also an element of Y and therefore $f(a) = 0$. Thus $f \in I(X)$.

   Let $a \in V(J)$. Then for all $f \in I \subseteq J$, $f(a) = 0$. Thus $a \in V(I)$.

Chapter 10

Introduction to Module Theory

10.1 Basic Definitions and Examples

In these exercises R is a ring with 1 and M is a left R-module.

1. These statements are all equivalent to the module being unital. Indeed,

$$\begin{aligned} 1m = m &\iff (0+1)m = m \iff 0m + 1m = m \iff 0m + m = m \iff 0m = 0 \\ &\iff (-1+1)m = 0 \iff (-1)m + m = 0 \iff (-1)m = -m. \end{aligned}$$

2. Take $r, s \in R^\times$ and some $m \in M$. Then $r(sm) = (rs)m$ because r and s are also in R. This shows that the first axiom of a group action is satisfied. Now since R has a 1, take $1 \in R^\times$. Again, it is easy to see that $1m = m$ and thus the second axiom of a group action is satisfied.

3. Suppose there exists some $s \in R$ such that $sr = 1$. Then $(sr)m = 1m = m$. But we also have $(sr)m = s(rm) = s0 = 0$. Thus $m = 0$, which is contrary to the assumption that m is nonzero. Thus r cannot have an inverse.

Note: for any $r \in R$, $r0 = r(0+0) = r0 + r0 \iff r0 = 0$.

4.

1. Let $N = \{(x_1, x_2, \dots, x_n) \mid x_i \in I_i\}$. An ideal of R is also a subgroup of R: thus it contains 0. This means that $(0, \dots, 0) \in N$; hence N is not empty. Take any $x, y \in N$ and any $\alpha \in R$. Then $x + \alpha y = (x_1 + \alpha y_1, x_2 + \alpha y_2, \dots, x_n + \alpha y_n) \in N$ because each I_i is closed under addition and left multiplication by an element of R. By the Submodule Criterion, N is a submodule of M.
2. Let $N = \{(x_1, x_2, \dots, x_n) \mid x_i \in I_i \text{ and } x_1 + x_2 + \cdots + x_n = 0\}$. The proof goes exactly as the last one, except we need to check the sum. We have that $(x_1 + \alpha y_1) + (x_2 + \alpha y_2) + \cdots + (x_n + \alpha y_n) = (x_1 + x_2 + \cdots + x_n) + \alpha(y_1 + y_2 + \cdots + y_n) = 0 + \alpha 0 = 0$.

5. It is clear that $0 \in IM$, hence IM is not empty. Without loss of generality, we can take $a_1m_1 + a_2m_2 + \cdots + a_nm_n$ and $b_1m_1 + b_2m_2 + \cdots + b_nm_n$ two elements of IM. Take also $\alpha \in R$. Then

$$\sum_{i=1}^n a_i m_i + \alpha \sum_{i=1}^n b_i m_i = \sum_{i=1}^n \underbrace{(a_i + \alpha b_i)}_{\in I} m_i \in IM.$$

Therefore by the Submodule Criterion IM is a submodule of M.

6. Let $\{M_i\}_{i \in I}$ be a nonempty collection of submodules of an R-module. From a result of group theory, we know $M = \bigcap_{i \in I} M_i$ is a subgroup: what's left to check is that M is closed under the action of R. Take some $m \in M$. Then $m \in M_i$ for all $i \in I$. Take some $\alpha \in R$. Because each M_i is a module, $\alpha m \in M_i\ \forall i \in I$. Hence $\alpha m \in M$, proving that M is a submodule of an R-module.

7. Let $N = \bigcup_{i=1}^{\infty} N_i$. It is evident that N is nonempty. Pick $x, y \in N$ and $\alpha \in R$. There exists some integers k, l such that $x \in N_k$ and $y \in N_l$. Without loss of generality, suppose $k \leq l$. Then $N_k \subseteq N_l$, which means that $x \in N_l$. Because N_l is a module, $x + \alpha y \in N_l \subseteq N$. By the Submodule Criterion, N is a submodule of M.

8.

1. It is easy to see that $0 \in \text{Tor}(M)$. Therefore $\text{Tor}(M) \neq \varnothing$. Now let $m, n \in \text{Tor}(M)$ and $\alpha \in R$. There exists nonzero elements r, s of R such that $rm = sn = 0$. Thus $rs(m + \alpha n) = (rs)m + (rs\alpha)n = s(rm) + r\alpha(sn) = s0 + r\alpha 0 = 0$. Since R is an integral domain, the product rs is nonzero. Therefore $m + \alpha n \in \text{Tor}(M)$. By the submodule criterion, $\text{Tor}(M)$ is a submodule of M.

2. Notice that the torsion elements in the R-module R are simply the zero divisors of R plus the zero element. Now consider the ring $\mathbb{Z}_6$ as a module over itself. In this module, 2 and 3 are torsion elements. However $2 + 3 = 5$ is not a torsion element because 5 is coprime with 6. Therefore $\text{Tor}(\mathbb{Z}_6)$ is not a subgroup (and thus not a submodule) of $\mathbb{Z}_6$.

3. Take nonzero elements a, b in R such that $ab = 0$. Take some nonzero $m \in M$. If $bm = 0$, then m is a torsion element and we are done. Else, $a(bm) = (ab)m = 0m = 0$ and bm is a torsion element. In both cases, $\text{Tor}(M)$ is not trivial so the statement is proven.

9. Write $I = \{r \in R \mid rn = 0\ \forall n \in N\}$ and take $a, b \in I$. Then, for any $n \in N$, $(a + b)n = an + bn = 0$, i.e. $a + b \in I$. Now take any $r \in R$. Firstly, $(ra)n = r(an) = r0 = 0$. Secondly, $(ar)n = a(rn)$. Since $rn \in N$ because N is a submodule, and since $a \in I$, we have that $a(rn) = 0$. Thus I absorbs multiplication by elements of R on the left and on the right: it is a 2-sided ideal of R.

10. Write $A = \{m \in M \mid am = 0\ \forall a \in I\}$. Since it is clear that $0 \in A$, we know that $A \neq \varnothing$. Take $m, n \in A$ and $r \in R$. For all $a \in I$, we have that $a(m + bn) = am + a(bn) = (ab)n$. Since I is a right ideal of R, $ab \in I$. Thus $(ab)n = 0$, meaning that $m + bn \in A$. By the submodule criterion, A is a submodule of M.

10.2 Quotient Modules and Module Homomorphisms

1. Let M and N be R-modules and let $\varphi : M \to N$ be a R-module homomorphism. It is clear that $0 \in \ker \varphi$, so it is not empty. Take any $x, y \in \ker \varphi$ and any $r \in R$. Then $\varphi(x + ry) = \varphi(x) + r\varphi(y) = 0$ and so $x + ry \in \ker \varphi$. By the submodule criterion, we get that $\ker \varphi$ is a submodule of M. Similarily, we see that $\operatorname{im} \varphi$ is not empty because it contains 0. Take any $x, y \in \operatorname{im} \varphi$ and any $r \in R$. Then there exists $a, b \in M$ such that $\varphi(a) = x$ and $\varphi(b) = y$. Thus $\varphi(a) + r\varphi(b) = \varphi(a + rb) = x + ry$ and we get by the submodule criterion that $\operatorname{im} \varphi$ is a submodule of N.

12. The notation in this question seems confusing at first, but realize that $I(R^n)$ and $(IR)^n$ are actually exactly the same thing (and this thing is an R-submodule of R^n).

We have by Exercise 5 in Section 1 that IR is a R-submodule of R. Therefore, by Exercise 11 of this section, we obtain the result immediatly.

10.3 Generation of Modules, Direct Sums and Free Modules

1. Notice that a homomorphism Φ from a free module $F(A)$ to a free module $F(B)$ is necessarily injective. Indeed, if $\sum \alpha_i a_i, \sum \beta_i a_i \in \ker \Phi$, then $\Phi(\sum \alpha_i a_i) = \sum \alpha_i \Phi(a_i) = 0$ and $\Phi(\sum \beta_i a_i) = \sum \beta_i \Phi(a_i) = 0$. Since $F(B)$ is a free module, $0 \in F(B)$ has a unique representation, meaning that $\alpha_i = \beta_i$ for each i.

Since A and B are sets of the same cardinality, there exists a bijection β between them. Let i and j be inclusion of A in $F(A)$ and of B in $F(B)$ respectively. By Theorem 6, we obtain a unique homomorphism $\Phi : F(A) \to F(B)$ such that $\Phi \circ i = j \circ \beta$. By the previous paragraph, it is a monomorphism. Now take any element $y = \sum \alpha_i (j \circ \beta)(a_i) \in F(B)$. By definition of Φ, we have $\Phi(\sum \alpha_i a_i) = \sum \alpha_i (j \circ \beta)(a_i) = y$ and so Φ is surjective. Hence it is an isomorphism and $F(A) \cong F(B)$.

2. Let I be a maximal ideal of R (such a maximal ideal always exists by Zorn's Lemma). Then by Exercise 12 of Section 2, $R^n/IR^n = R^n/I^n \cong (R/I) \times \cdots \times (R/I)$ (n times) and similarily $R^m/IR^m \cong (R/I) \times \cdots \times (R/I)$ (m times). By maximality of I, $R/I = K$ is a field. Thus we get $R^n \cong R^m$ if and only if $K^n \cong K^m$ if and only if $n = m$.

3.

1. Consider the $\mathbb{R}[x]$-module M induced from the vector space $\mathbb{R}^2$ over the field $\mathbb{R}$ using the linear transformation T which sends a vector to its counter-clockwise rotation by $\pi/2$ radians. Take $(1,0) \in \mathbb{R}$: this element is a generator for M. Indeed, take any $(a,b) \in \mathbb{R}^2$. Then $(a+bx)\cdot(1,0) = a\cdot(1,0) + b\cdot T(1,0) = a(1,0) + b(0,1) = (a,b)$, hence $\mathbb{R}[x]\cdot(1,0) = M$. Therefore M is a cyclic module.

2. Consider a similar M again but this time induced using the linear transformation T' which is a projection on the y-axis. The element $(1,1) \in \mathbb{R}^2$ generates M: take any $(a,b) \in \mathbb{R}^2$. Then $(a+(b-a)x)\cdot(1,1) = a(1,1)+(b-a)T'(1,1) = a(1,1)+(b-a)(0,1) = (a,a)+(0,b-a) = (a,b)$. Thus M is a cyclic module.

9. Suppose that $M \neq 0$ and M is a cyclic module with any nonzero element as generator. Take $N \neq 0$ a submodule of M and pick some $n \in N$. Then $Rn \subseteq N$ as N is closed under the action of R. Moreover $Rn = M$ by our supposition. Hence $M = N$. Because N was aribtrary, we conclude that M is irreducible. On the other hand, suppose that M is irreducible (and so $M \neq 0$). Take any nonzero $m \in M$. Then Rm is a submodule of M, hence by irreducibility $Rm = M$ and m is a generator of M.

Because $\mathbb{Z}$-modules are the same thing as abelian groups and $\mathbb{Z}$-submodules are the same thing as subgroups of abelian groups, the irreducible $\mathbb{Z}$-modules are exactly the simple abelian groups. By basic group theory, these are exactly the abelian groups having order a prime number.

11. **Schur's Lemma**. Take M_1 and M_2 irreducible R-modules and $\varphi \in \mathrm{Hom}_R(M_1, M_2)$ with φ nonzero. Since $\ker \varphi$ is a submodule of M_1 and $\ker \varphi \neq M_1$, we must have $\ker \varphi = 0$. Similarily, since $\mathrm{im}\, \varphi$ is a submodule of M_2 and $\mathrm{im}\, \varphi \neq 0$, we must have $\mathrm{im}\, \varphi = M_2$. Thus $M_1 \cong M_2$. Now consider some $\alpha \in \mathrm{End}_R(M)$ for M an irreducible R-module. By the previous result, α must be an automorphism or the zero homomorphism; in the first case it always has an inverse. Therefore $\mathrm{End}_R(M)$ is a divison ring.

Chapter 11

Vector Spaces

11.1 Definitions and Basic Theory

1. Suppose $(a_1, a_2, \dots, a_n)$ is not the zero vector. Let $\varphi : \mathbb{R}^n \to \mathbb{R}$ be given by $\varphi(x_1, x_2, \dots, x_n) = a_1x_1 + a_2x_2 + \cdots + a_nx_n$. This is a linear mapping because

$$\begin{aligned}\varphi((x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n)) &= a_1(x_1 + y_1) + a_2(x_2 + y_2) + \cdots + a_n(x_n + y_n)\\ &= (a_1x_1 + a_2x_2 + \cdots + a_nx_n) + (a_1y_1 + a_2y_2 + \cdots + a_ny_n)\\ &= \varphi(x_1, x_2, \dots, x_n) + \varphi(y_1, y_2, \dots, y_n)\end{aligned}$$

and

$$\begin{aligned}\varphi(\alpha(x_1, x_2, \dots, x_n)) &= a_1(\alpha x_1) + a_2(\alpha x_2) + \cdots + a_n(\alpha x_n)\\ &= \alpha(a_1x_1 + a_2x_2 + \cdots + a_nx_n)\\ &= \alpha\varphi(x_1, x_2, \dots, x_n).\end{aligned}$$

It is clear that φ is surjective: pick any $y \in \mathbb{R}$. Without loss of generality, $a_1 \neq 0$, hence $y = \varphi((y/a_1), 0, \dots, 0)$. Thus $\dim \operatorname{im} \varphi = 1$. By Corollary 8, we get that $\dim \ker \varphi = n-1$. Since the kernel of φ is the set of elements $(x_1, x_2, \dots, x_n)$ of $\mathbb{R}^n$ with $a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$ and $\ker \varphi$ is a subspace of $\mathbb{R}^n$, this answers the first part of the question.

To find a base, let

$$B = \left\{ b_2 = \left(\frac{-a_2}{a_1}, 1, 0, \dots, 0\right), b_3 = \left(\frac{-a_3}{a_1}, 0, 1, \dots, 0\right), \dots, b_n = \left(\frac{a_n}{a_1}, 0, 0, \dots, 1\right) \right\}$$

(recall that $a_1 \neq 0$). Pick any vector $x = (x_1, x_2, \dots, x_n) \in \ker \varphi$. Then $x_1 = (-1/a_1)(a_2x_2 + \cdots + a_nx_n)$, hence $x = x_2b_2 + x_3b_3 + \cdots + x_nb_n$. Thus B spans $\ker \varphi$. Moreover it is easy to see that B is a linearly independent set. Therefore it is a basis (of $n-1$ elements) for the vector subspace $\ker \varphi$.

3. Let $b_1 = (1, 0, 0, 0)$, $b_2 = (1, -1, 0, 0)$, $b_3 = (1, -1, 1, 0)$ and $b_4 = (1, -1, 1, -1)$. Then, $(0, 1, 0, 0) = b_2 - b_1$, $(0, 0, 1, 0) = b_3 - b_2$ and $(0, 0, 0, 1) = b_3 - b_4$. Therefore

$$\begin{aligned}\varphi((a, b, c, d)) &= \varphi(ab_1 + b(b_2 - b_1) + c(b_3 - b_2) + d(b_3 - b_4))\\ &= (a-b)\varphi(b_1) + (b-c)\varphi(b_2) + (c+d)\varphi(b_3) + d\varphi(b_4)\\ &= a - b + c + d.\end{aligned}$$

This is a concrete realization of an ”extension by linearity” of φ.