Dummit and Foote - Abstract Algebra
Answers to Selected Exercises

Marc-André Brochu

Winter 2019

Chapter 7

Introduction to Rings

7.1 The Chinese Remainder Theorem

6. Write $f_i(x) = c_{i0} + c_{i1}x + c_{i2}x^2 + \cdots + c_{id}x^d$ for each $i = 1, 2, \ldots, k$. We wish to exhibit a polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ such that for every $m = 0, 1, \ldots, d$, we have that $a_m \equiv c_{im} \bmod n_i$ for every $i = 1, 2, \ldots, k$, i.e. we want the coefficients of f to agree (mod n_i) with the coefficients of f_i for each i.

By the Chinese Remainder Theorem, because the n_i's are pairwise coprime, $\mathbb{Z}/(n_1n_2 \ldots n_k)\mathbb{Z}$ is isomorphic to $S = \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$. Hence for a fixed $m \in \{0, 1, \ldots, d\}$ and for $s = (c_{1m}, c_{2m}, \ldots, c_{km}) \in S$, there is a unique residue $a_m \in \mathbb{Z}/(n_1n_2 \ldots n_k)\mathbb{Z}$ that maps to it. We "lift" the residue into $\mathbb{Z}$ as a_m and we use that integer for the correspondingly named coefficient in $f(x)$.

If the polynomials $f_i(x)$ are all monic, then by doing the same procedure as in the previous paragraph we will find that the element $(1, 1, \ldots, 1) \in S$ corresponding to the coefficients of the highest degree in the $f_i(x)$'s have to be the (isomorphic) image of the residue $1 \in \mathbb{Z}/(n_1n_2 \ldots n_k)\mathbb{Z}$. This is because the isomorphism to S is an isomorphism of rings, hence it must preserve the multiplicative identity. Therefore we can lift the residue $1 \in \mathbb{Z}/(n_1n_2 \ldots n_k)\mathbb{Z}$ to the integer $1 \in \mathbb{Z}$ and use that as the highest coefficient in $f(x)$, meaning that it is possible to choose $f(x)$ to be a monic polynomial.

Chapter 8

Euclidean Domains, Principal Ideal Domains and Unique Factorization Domains

8.1 Euclidean Domains

7.

(a) Set $\alpha = a + bi$ and $\beta = c + di$. We simply have

$$\frac{\alpha}{\beta} = \frac{a+bi}{c+di} \cdot \frac{c-di}{c-di} = \underbrace{\left(\frac{ac+bd}{c^2+d^2}\right)}_{r} + \underbrace{\left(\frac{bc-ad}{c^2+d^2}\right)}_{s} \cdot i$$

and obviously $r, s \in \mathbb{Q}$. Also notice that this means $\alpha = \beta(r + si)$.

(b) Because p is an integer closest to r, we must have $|r - p| \leq 1/2$. Similarly, $|s - q| \leq 1/2$. Hence $(r-p)^2 \leq 1/4$ and $(s-q)^2 \leq 1/4$, so $N(\theta) \leq 1/4 + 1/4 = 1/2$. Consider $\gamma = \beta\theta$. We have $\beta\theta = \beta(r-p) + \beta(s-q)i = \beta(r+si) - \beta(p+qi)$. Hence by (a) we obtain $\gamma = \alpha - (p+qi)\beta$ and so $\gamma \in \mathbb{Z}[i]$. Moreover, $N(\gamma) = N(\beta)N(\theta) \leq \frac{1}{2}N(\beta)$. Therefore $\alpha = (p+qi)\beta + \gamma$ with $N(\gamma) < N(\beta)$, which gives a division algorithm for $\mathbb{Z}[i]$ (division of α by $\beta \neq 0$).

(c) We will compute a greatest common divisor of 85 and $1 + 13i$. First, we compute

$$\frac{85}{1+13i} = \frac{85}{1+13i} \cdot \frac{1-13i}{1-13i} = \frac{1-13i}{2}$$

to get that $r = 1/2$ and $s = -13/2$. Take $p = 0$ and $q = -6$. So $\theta = (1/2) - (1/2)i$ and $\gamma = (1+13i)(1-i)/2 = 7+6i$. So $85 = (-6i)(1+13i) + (7+6i)$, which gives the first step of the Euclidean Algorithm. Since the rest is non-zero, we must continue the algorithm by computing the rest of $1 + 13i$ divided by $7 + 6i$. Happily,

$$\frac{1+13i}{7+6i} = \frac{1+13i}{7+6i} \cdot \frac{7-6i}{7-6i} = 1 + i$$

and so this step already gives us that $1 + 13i = (1+i)(7+6i) + 0$. Because the rest is zero, we stop the algorithm here: a greatest common divisor of 85 and $1 + 13i$ is $7 + 6i$.

8.2 Principal Ideal Domains

8.3 Unique Factorization Domains

1. Write $\alpha = xy$ for $x, y \in \mathbb{Z}[\sqrt{D}]$ and suppose that $N(\alpha) = \pm p$ for p a prime number in $\mathbb{Z}$. Then $N(\alpha) = N(x)N(y)$ and so $N(x)N(y) = \pm p$. Obviously this means that either $N(x)$ or $N(y)$ is ± 1 (this is technically because $\mathbb{Z}$ is an integral domain, so any prime element is also irreducible and the only units in $\mathbb{Z}$ are ± 1). Without loss of generality $N(x) = \pm 1$, hence x is a unit in $\mathbb{Z}[\sqrt{D}]$. Therefore α is irreducible in $\mathbb{Z}[\sqrt{D}]$.

2.

(a) We have that α is a unit in $\mathbb{Z}[i]$ if and only if $N(\alpha) = \pm 1$. Since we are working with $D = -1$, the norm is always non-negative, hence $\alpha = a + bi$ is a unit if and only if $N(a + bi) = a^2 + b^2 = 1$. We can see easily that this is the case only when $a = \pm 1$ or $b = \pm 1$ (and only one of a, b is nonzero at a time). Thus the units in the Gaussian integers are exactly ± 1 and $\pm i$.

(b) Notice that $N(a \pm bi) = (a + bi)(a - bi)$. Thus $(1 + i)(1 - i) = N(1 \pm i) = 2$ and by the previous problem (3.1), we conclude that both $1 + i$ and $1 - i$ are irreducible (because 2 is prime), and also that the equality we were tasked to verify holds. For exactly the same reasons, $5 = 2^2 - 2i + 2i - i^2 = (2 + i)(2 - i) = N(2 \pm i)$ with $2 + i$ and $2 - i$ irreducible elements of $\mathbb{Z}[i]$.

Now let's show that 3 is irreducible. Write $3 = ab$. Then $N(3) = 9$ and also $N(3) = N(a)N(b)$. The divisors of 9 are ± 1, ± 3 and ± 9 (in $\mathbb{Z}$) and $N(a)$, $N(b)$ are *positive* divisors of 9. Suppose $N(a) = N(b) = 3$. Write $a = x + yi$ for integers x and y. Then $N(a) = x^2 + y^2 = 3$ and so $x^2 + y^2 \equiv 3 \bmod 4$. This is a problem because the only squares mod 4 are 0 and 1: as a result $x^2 + y^2$ can only take the values 0, 1 or 2 mod 4. Therefore it is never possible to have $N(a) = N(b) = 3$, hence one of $N(a)$ or $N(b)$ is 1 or 9. In that case, it is easy to see that the other divisor must be 9 or 1 respectively, giving that 3 is irreducible in $\mathbb{Z}[i]$ (recall that a is a unit in $\mathbb{Z}[i]$ iff $N(a) = 1$).

We work in a similar way to show that 7 is irreducible. Write $7 = ab$. Then $N(a)N(b) = 49$. Suppose $N(a) = N(b) = 7$ and write $a = x + yi$. Then $x^2 + y^2 = 7$ and so $x^2 + y^2 \equiv 3 \bmod 4$. For the same reasons as above, this gives that 7 is irreducible in $\mathbb{Z}[i]$.

(c) We notice a pattern: it seems that if p is a prime (in $\mathbb{Z}$) such that $p \equiv 3 \bmod 4$, then p is irreducible in $\mathbb{Z}[i]$. Let us prove this. Write $p = ab$ for $a, b \in \mathbb{Z}[i]$. We have $N(p) = p^2$ and $N(p) = N(a)N(b)$. The positive divisors of p^2 (and so the possible values for $N(a)$ and $N(b)$ in our situation) are 1, p and p^2. Suppose that $N(a) = N(b) = p$ and write $a = x + yi$. Then $x^2 + y^2 \equiv p \equiv 3 \bmod 4$, which is impossible because the squares mod 4 are 0 and 1, meaning the sum of two squares cannot be 3. Therefore one of $N(a)$ and $N(b)$ must be 1 and thus one of a and b must be a unit. Hence p is irreducible in the Gaussian integers.

This immediately gives us that 11, 19, 23 and 31 are irreducibles in $\mathbb{Z}[i]$.

We also see that if some $a \in \mathbb{Z}$ is the sum of two squares, then $a = x^2 + y^2 = (x + yi)(x - yi)$ and so a is reducible in $\mathbb{Z}[i]$. Because $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$ and $29 = 2^2 + 5^2$, these are reducible.

Chapter 9

Polynomial Rings

9.1 Definitions and Basic Properties

12. First, notice that in R, the ideal (x,z) is equal to the ideal $(x,z,xy-z^2)$. This is pretty easy to see but we will prove it explicitely. Clearly, $(x,z) \subseteq (x,z,xy-z^2)$. Now take some $a \in (x,z,xy-z^2)$. Then $a = r_1x + r_2z + r_3xy - r_3z^2$ for some $r_1, r_2, r_3 \in R$. Hence $a = (r_1 + r_3y)x + (r_2 + r_3z)z \in (x,z)$. Therefore $(x,z,xy-z^2) = (x,z)$.

Let $I = (xy-z^2)$ and $J = (x,z,xy-z^2) = (x,z)$. We have that $I \subset J$. By the Third Isomorphism Theorem for Rings (p.246 of D&F), we get that $J/I = (\overline{x}, \overline{z}) = \overline{P}$ is an ideal of $R/I = \overline{R}$ (we already knew that) and crucially,

$$\overline{R}/\overline{P} \cong R/J = \mathbb{Q}[x,y,z]/(x,z) \cong \mathbb{Q}[y].$$

Because $\mathbb{Q}[y]$ is an integral domain, we conclude that the ideal $\overline{P}$ of $\overline{R}$ must be a prime ideal.

Since $\overline{P}^2 = \{\overline{\alpha} \cdot \overline{\gamma} \mid \overline{\alpha}, \overline{\gamma} \in \overline{P}\}$, it is clear that $\overline{xy} = \overline{z} \cdot \overline{z} \in \overline{P}^2$. Now suppose that there exists some integer $k \geq 0$ such that $\overline{y}^k \in \overline{P}^2$. This means that $\overline{y}^k = \overline{\alpha} \cdot \overline{\gamma}$ for some $\overline{\alpha}, \overline{\gamma} \in \overline{P}$. Let $\pi : \overline{R} \to \overline{R}/\overline{P}$ be the natural projection homomorphism. Then $\pi(\overline{y}^k) = \pi(\overline{y})^k = 0$. However $\pi(\overline{y})$ is nonzero. This is in contradiction with the fact that $\mathbb{Q}[y]$, to which $\overline{R}/\overline{P}$ is isomorphic, is an integral domain. Therefore no power of $\overline{y}$ lies in $\overline{P}^2$.

9.2 Poynomial Rings Over Fields I

9.3 Polynomial Rings that are Unique Factorization Domains

2.

(a) We apply Eisenstein's Criterion with prime $p = 2$. We can apply the criterion because 2 divides both -4 and 6, but happily $p^2 = 4$ does not divide 6 and thus $x^4 - 4x^3 + 6$ is irreducible in $\mathbb{Z}[x]$.

(b) This is another direct application of Eisenstein's Criterion, using prime $p = 3$. Indeed, 3 divides all of 30, -15, 6 and -120 while $p^2 = 9$ fails to divide 120. Hence $x^6 + 30x^5 - 15x^3 + 6x - 120$ is irreducible in $\mathbb{Z}[x]$.

(c) Let $f(x) = x^4 + 4x^3 + 6x^2 + 2x + 1$. It seems we cannot apply Eisenstein's Criterion directly, but following the hint in the question we let $g(x) = f(x-1)$. After computation, we get that $g(x) = x^4 - 2x + 2$. We apply Eisenstein's Criterion with prime $p = 2$ on $g(x)$ to obtain that $g(x)$ is irreducible in $\mathbb{Z}[x]$. This means that $f(x)$ is also irreducible: if it were not, then the reduction $f(x) = a(x)b(x)$ would make $g(x)$ reducible because we would have $g(x) = a(x-1)b(x-1)$.

(d) We compute

$$f(x) = \frac{(x+2)^p - 2^p}{x} = \sum_{k=1}^{p} \binom{p}{k} x^{k-1} 2^{p-k} = p\, 2^{p-1} + x^{p-1} + \sum_{k=2}^{p-1} \binom{p}{k} x^{k-1} 2^{p-k}$$

and we can now see that the prime integer p divides every coefficient of $f(x)$ except the leading one (which is 1, i.e. this polynomial is monic). Moreover, because p is odd, we see that p^2 cannot divide $p\, 2^{p-1}$. Therefore, by the Eisenstein Criterion, $f(x)$ is irreducible in $\mathbb{Z}[x]$.

9.4 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. $f = f_1 j_1 + \cdots + f_n j_n$ with $f_i \in R$, $j_i \in J$ and $n \in \mathbb{N}$. So $f(a) = f_1(a) j_1(a) + \cdots + f_n(a) j_n(a)$. 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.

(a) Let $N = \{(x_1, x_2, \ldots, x_n) \mid x_i \in I_i\}$. An ideal of R is also a subgroup of R: thus it contains 0. This means that $(0, \ldots, 0) \in N$; hence N is not empty. Take any $x, y \in N$ and any $\alpha \in R$. Then $x + \alpha y = (x_1 + \alpha y_1, x_2 + \alpha y_2, \ldots, x_n + \alpha y_n) \in N$ 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.

(b) Let $N = \{(x_1, x_2, \ldots, x_n) \mid x_i \in I_i \text{ and } x_1 + x_2 + \cdots + x_n = 0\}$. 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.

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

(b) Notice that the torsion elements in the R-module R are simply the zero divisors of R plus the zero element. For instance, consider the ring $\mathbb{Z}_6$ as a module over itself. Its zero divisors (torsion elements) are $\{0, 2, 3, 4\}$, and so it is clear that $\mathrm{Tor}(\mathbb{Z}_6)$ fails to be a group: $2 + 3 = 5$ is not a torsion element because 5 is coprime with 6 and hence is not a zero divisor. Therefore $\mathrm{Tor}(\mathbb{Z}_6)$ is not a submodule of $\mathbb{Z}_6$.

(c) 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, $\mathrm{Tor}(M)$ 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 $\mathrm{im}\, \varphi$ is not empty because it contains 0. Take any $x, y \in \mathrm{im}\, \varphi$ 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 $\mathrm{im}\, \varphi$ is a submodule of N.

8. Pick some element $x \in \mathrm{Tor}(M)$. Then there exists some nonzero $r \in R$ such that $rx = 0$. Hence $\varphi(rx) = r\varphi(x) = 0$ because φ is a homomorphism and thus preserves the action of r and maps 0_M to 0_N. This means that $\varphi(x) \in \mathrm{Tor}(N)$ (the element of R that annihilates x in M also annihilates $\varphi(x)$ in N). Therefore $\varphi(\mathrm{Tor}(M)) \subseteq \mathrm{Tor}(N)$.

9. Following the hint in the text, we wish to show that each $\varphi \in \mathrm{Hom}_R(R, M)$ is completely determined by its value at $1 \in R$. This is easy to see: $\varphi(r) = \varphi(r \cdot 1) = r\varphi(1)$ for all $r \in R$ (the action of R on itself as a module is just multiplication). This means that two different

$\varphi,\ \nu \in \operatorname{Hom}_R(R, M)$ will have $\varphi(1) \neq \nu(1)$. Hence the map $f : \operatorname{Hom}_R(R, M) \to M$ given by $f(\varphi) = \varphi(1)$ is injective.

To show that the map f is surjective, take any $m \in M$ and consider the mapping $\varphi_m : R \to M$ given by $\varphi_m(r) = rm$. It is easy to see that this mapping is a homomorphism between R-modules. Let us check just to be sure: if we have $x, y, \alpha \in R$, then $\varphi_m(\alpha x+y) = (\alpha x+y)m = (\alpha x)m+ym = \alpha(xm)+ym = \alpha\varphi_m(x)+\varphi_m(y)$, which verifies our claim. Moreover, $f(\varphi_m) = \varphi_m(1) = 1m = m$. This shows that $\operatorname{im} f = M$.

Now we need to show that f is a (R-module) homomorphism. Because it is a bijection by the preceding two paragraphs, this will prove that $\operatorname{Hom}_R(R, M) \cong M$. Take $\alpha \in R$ and $\varphi, \nu \in \operatorname{Hom}_R(R, M)$. Then $f(\alpha\varphi+\nu) = (\alpha\varphi+\nu)(1) = (\alpha\varphi)(1)+\nu(1) = \alpha(\varphi(1))+\nu(1) = \alpha f(\varphi)+f(\nu)$. Hence f is an (R-module) isomorphism. This finishes the answer to the question.

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

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.

(a) 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.

(b) 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.

7. Take $A = \{\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}\}$ to be a generating set for M/N and $B = \{b_1, b_2, \ldots, b_m\}$ to be a generating set for N. Pick any element $m \in M$. We will show that this element can be written using only the (finite number of) generators in $A \cup B$. This will show that M is a finitely generated module.

As usual, $\overline{m}$ denotes the projection of m inside M/N. We have that $\overline{m} = r_1\overline{a_1}+r_2\overline{a_2}+\cdots+r_n\overline{a_n} = \overline{r_1a_1 + r_2a_2 + \cdots + r_na_n}$. This holds if and only if $m - (r_1a_1 + r_2a_2 + \cdots + r_na_n) \in N$, and so $m-(r_1a_1+r_2a_2+\cdots+r_na_n) = s_1b_1+s_2b_2+\cdots+s_mb_m$. Hence $m = r_1a_1+r_2a_2+\cdots+r_na_n+ s_1b_1 + s_2b_2 + \cdots + s_mb_m$. Because m was arbitrary, this proves the claim that M is a finitely generated module and $M = R(A \cup B)$.

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 $\operatorname{im} \varphi$ is a submodule of M_2 and $\operatorname{im} \varphi \neq 0$, we must have $\operatorname{im} \varphi = M_2$. 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 $(a_1, a_2, \ldots, a_n)$ is not the zero vector. Let $\varphi : \mathbb{R}^n \to \mathbb{R}$ be given by $\varphi(x_1, x_2, \ldots, x_n) = a_1x_1 + a_2x_2 + \cdots + a_nx_n$. This is a linear mapping because

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

and

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

It is clear that φ is surjective: pick any $y \in \mathbb{R}$. Without loss of generality, $a_1 \neq 0$, hence $y = \varphi((y/a_1), 0, \ldots, 0)$. 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 $(x_1, x_2, \ldots, x_n)$ 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

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

(recall that $a_1 \neq 0$). Pick any vector $x = (x_1, x_2, \ldots, x_n) \in \ker \varphi$. 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.

11.2 The Matrix of a Linear Transformation

11.

(a) Take $y \in \operatorname{im}\varphi \cap \ker\varphi$. Then there is some $x \in V$ such that $\varphi(x) = y$ and moreover $\varphi(y) = 0$. Since $\varphi(y) = \varphi^2(x)$ and $\varphi = \varphi^2$, we must have $\varphi(y) = \varphi(x) = 0$. Hence $y = 0$ by the first equality. Because y was arbitrary, we must have $\operatorname{im}\varphi \cap \ker\varphi = 0$.

(b) Take any $x \in V$. The intuition here is that since φ is idempotent, the natural projection $\pi : V \to V/\ker\varphi$ will map x and $\varphi(x)$ to the same element, because x and $\varphi(x)$ will basically "collapse" to the same element of V. More precisely, we have that $\varphi(x) = \varphi^2(x)$ and thus $\varphi(x-\varphi(x)) = 0$, or in other words $x-\varphi(x) \in \ker\varphi$. Now $x = \varphi(x)+[x-\varphi(x)] \in \operatorname{im}\varphi+\ker\varphi$. Because x was arbitrary, we get that $V = \operatorname{im}\varphi + \ker\varphi$. Since $\operatorname{im}\varphi$ and $\ker\varphi$ are both submodules of the F-module V, we get by (a) and by Proposition 5 (on p.329 of D&F) that $V = \operatorname{im}\varphi \oplus \ker\varphi$.

(c) Let $\mathcal{B} = \{u_1, u_2, \ldots, u_k\}$ be a basis for $\operatorname{im}\varphi$ and let $\mathcal{C} = \{v_1, v_2, \ldots, v_l\}$ be a basis for $\ker\varphi$. By (b), we know that any $x \in V$ can be written uniquely as $x = \alpha + \beta$ for $\alpha \in \operatorname{im}\varphi$ and $\beta \in \ker\varphi$. Therefore any $x \in V$ can also be written uniquely as $x = (a_1u_1 + a_2u_2 + \cdots + a_ku_k) + (b_1v_1 + b_2v_2 + \cdots + b_lv_l)$ for $a_i, b_i \in F$. This means that the set $\{u_1, u_2, \ldots, u_k, v_1, v_2, \ldots, v_l\} = \mathcal{D}$ spans V; moreover the uniqueness signifies that $\mathcal{D}$ is actually a set of independent vectors. Hence $\mathcal{D}$ is a basis for V.

Now let u_i be one of the basis element of $\operatorname{im}\varphi$ in $\mathcal{B}$. Then there exists some $w \in V$ such that $\varphi(w) = u_i$. Using idempotence, $\varphi(w) = \varphi(u_i) = u_i$. Therefore, in the matrix representation of φ, in the column standing for the basis element u_i, there is a single 1 on the ith row and zeros everywhere else, for i ranging from 1 to $\dim(\operatorname{im}\varphi)$.

If v_i is one of the basis element of $\ker\varphi$ in $\mathcal{C}$, then obviously $\varphi(v_i) = 0$ and as such the column standing for v_i in the matrix representation of φ is only zeroes (with i ranging from $\dim(\operatorname{im}\varphi) + 1$ to $\dim V$).

This shows that the matrix representation of φ is a diagonal matrix with only ones and zeroes in it.

35.

(a) Take any matrix $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in V. Then obviously $M = a\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) + b\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) + c\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) + d\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, hence these four matrices form a spanning set of V. It is also obvious that any smaller subset of these four matrices would not span V. Therefore they form a basis for V. As a consequence we have $\dim V = 4$.

(b) Let $\gamma \in \mathbb{R}$ and $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in V$. Then $\varphi(\gamma A) = \gamma a + \gamma d = \gamma(a + d) = \gamma\varphi(A)$. Now let $B = \left(\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right) \in V$. We have $\varphi(A+B) = (a+w)+(d+z) = (a+d)+(w+z) = \varphi(A)+\varphi(B)$. Hence φ is a linear transformation between V and $\mathbb{R}$.

Obviously $\mathbb{R}$ is a one-dimensional vector space with $\{1\}$ as a basis. Because $\varphi\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) = \varphi\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) = 1$ and $\varphi\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) = \varphi\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) = 0$, we get that the matrix representation of φ for these bases is given by $M = \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}$. Since φ is visibly surjective, we have $\dim\varphi(V) = \dim\mathbb{R} = 1$.

We know that $\dim V = \dim\varphi(V) + \dim(\ker\varphi)$, and thus $\dim(\ker\varphi) = 4 - 1 = 3$. Consider the set of matrices $\mathcal{B} = \{\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)\}$. These three matrices are clearly linearly independent. Because for any real numbers a, b, c we have $\varphi(a\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right) + b\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) + c\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)) = a\varphi(\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)) + b\varphi(\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)) + c\varphi(\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)) = 0$, this means that $\operatorname{Span}(\mathcal{B}) \subseteq \ker\varphi$. But $\ker\varphi$ has dimension three, as computed earlier. This means that $\mathcal{B}$ is actually a basis for $\ker\varphi$.

11.3 Dual Vector Spaces

4. Let $v^* : V \to K$ a linear functionnal of V^* be given by

$$v^*(v) = \sum_{a^* \in A^*} a^*(v).$$

This sum always has a value (in K) because only finitely many values in the sum are 1 (the rest are zeroes). It is easy to see that v^* cannot be written as a finite linear combination of elements of A^*. Thus $v^* \notin \operatorname{Span}(A^*)$. This means that $\dim V < \dim V^*$.