Solution Set 6

Math 123
March 18, 2002

1. *Artin §12.1 #1*

Let $\varphi : R \to R$ be a module homomorphism. Since the action of $r \in R$ on $x \in R$ is $r \cdot x = rx$, by the definition of a module homomorphism we have for any $r \in R$,

$$\varphi(r) = \varphi(r \cdot 1) = r\varphi(1).$$

Thus φ is determined by $\varphi(1)$ (in general, any module homomorphism $\varphi : R \to M$ for any R-module M is determined by $\varphi(1)$ for the same reason). It is easy to see that we can choose any value for $\varphi(1)$,[1] we have classified all module homomorphisms $R \to R$ as given by multiplication by some ring element.

---

2. *Artin §12.1 #5*

Suppose that $f(\alpha) = 0$ where $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$ is a monic irreducible integer polynomial. Then $1, \alpha, \ldots, \alpha^{n-1}$ generate R as a free $\mathbf{Z}$-module (i.e. $\alpha^n = -(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1})$), so $R \cong \mathbf{Z} \oplus \mathbf{Z}\alpha \oplus \cdots \oplus \mathbf{Z}\alpha^{n-1}$ as an abelian group, and $R/mR \cong (\mathbf{Z}/m\mathbf{Z})^n$ has m^n elements.

---

3. *Artin §12.1 #6*

a) Let N be a simple R-module, and let $n \in N$ be any nonzero element. The module generated by n (i.e. all finite sums $\sum_i r_i n$ for $r_i \in R$) is a submodule of N, so it must be all of N; thus N is generated (as an R-module) by n.

Define a module homomorphism $\varphi : R \to N$ given by $\varphi(1) = n$ (and $\varphi(r) = \varphi(r \cdot 1) = r \cdot n$). We know that $M = \ker\varphi$ is a submodule and thus an ideal of R, and since φ is surjective (since n generates N), by the First Isomorphism Theorem, $R/M \cong N$ (as R-modules). But R/M is also a ring, and its R-module structure is also given by ring multiplication. Since N and therefore R/M are simple, R/M has no proper submodules, i.e. no proper ideals, and is therefore M is maximal.

b) *Schur's Lemma*[2]

Suppose that φ is nonzero. Let s generate S and s' generate S'; note that we can take $s' = \varphi(s)$ since s generates S and φ is nonzero (so φ is surjective). Consider $M = \ker\varphi$.

[1] Most people forgot to note this, but the problem does state, "determine all module homomorphisms."
[2] Schur's Lemma is important in representation theory.

We know that M is a submodule of S, so either $M = 0$ or $M = S$. But $M \neq S$ since φ is nonzero, so φ is injective and is thus bijective.

---

4. *Artin §12.2 #1*

By the next problem, $M = (x, y)$ is free if and only if it is a principal ideal (note that $\mathbf{C}[x, y]$ is an integral domain and thus has no zero divisors). But we know that this is not the case.

---

5. *Artin §12.2 #5*

Suppose that I is a free R-module, so we have a module isomorphism $\varphi : R^n \to I$. Let $\epsilon_1, \ldots, \epsilon_n$ be the standard basis for R^n. Since I is a subset of the ring R, the expression $\varphi(\epsilon_i) \cdot \epsilon_j$ makes sense. Assume that $n > 1$. We have

$$\varphi(\varphi(\epsilon_2) \cdot \epsilon_1 - \varphi(\epsilon_1) \cdot \epsilon_2) = \varphi(\epsilon_2) \cdot \varphi(\epsilon_1) - \varphi(\epsilon_1) \cdot \varphi(\epsilon_2) = 0$$

but the $\{\epsilon_i\}$ form a basis for R^n and are thus linearly independent, so $\varphi(\epsilon_2) \cdot \epsilon_1 - \varphi(\epsilon_1) \cdot \epsilon_2 \neq 0$ since φ is injective. But this contradicts the assumption that φ is injective, so we must have $n = 1$. Thus $\epsilon_1 = 1$, and to say that $\varphi : R \to I$ is a module isomorphism is equivalent to saying that I is the principal ideal generated by $\alpha = \varphi(1)$. Now, if α is a zero divisor of R then there exists some nonzero $r \in R$ with $r\alpha = 0$, so $\varphi(r) = r\varphi(1) = r\alpha = 0$, which again contradicts the assumption that φ is injective. Thus α is not a zero divisor.

Conversely, suppose that $I = (\alpha)$ is the principal ideal generated by an element α which is not a zero divisor. Define $\varphi : R \to I$ by $\varphi(1) = \alpha$. Clearly φ is surjective; if $\varphi(r) = 0$ then $r\alpha = 0$, which means $r = 0$. Thus φ is a module isomorphism.

---

6. *Artin §12.2 #6*

Let R be a ring such that every finitely generated R-module is free, and assume that R is not the zero ring. Suppose that R has some proper ideal I, which contains a nonzero element r. Well, R/I is an R-module, so it is free; thus there is a module isomorphism $\varphi : R^n \to R/I$. But $\varphi(r, 0, \ldots, 0) = r \cdot \varphi(1, 0, \ldots, 0) = 0$ since $r = 0$ in R/I, which contradicts the fact that φ is injective. Thus R can have no proper ideals and is a field.

---

7. *Artin §12.3 #3*

Let $f(x_i) \in \mathbf{Z}[x_1, \ldots, x_n]$ be a polynomial identity[3] whose corresponding real polynomial function is $\tilde{f} : \mathbf{R}^n \to \mathbf{R}$. By Artin Chapter 10, Proposition 3.8, if $\tilde{f}$ is identically zero then

[3] Note that f is not necessarily a *matrix* identity.

$f = 0$ (this is the only important property of the real numbers that we use; the rest of the proof given in Artin for the complex numbers is identical). Thus the image of f under the canonical ring homomorphism $\mathbf{Z}[x_i] \to R[x_i]$ is zero, so the identity holds in R.

---

8. *Artin §12.4 #1*

a)

$$\begin{bmatrix} 3 & 1 \\ -1 & 2 \end{bmatrix} \to \begin{bmatrix} 0 & 7 \\ -1 & 2 \end{bmatrix} \to \begin{bmatrix} 0 & 7 \\ -1 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 0 \\ 0 & 7 \end{bmatrix}$$

b)

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 3 \\ 4 & -3 & 6 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 \\ 4 & -3 & -6 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 \\ 4 & -3 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \end{bmatrix}$$

c)

$$\begin{bmatrix} 3 & 1 & -4 \\ 2 & -3 & 1 \\ -4 & 6 & -2 \end{bmatrix} \to \begin{bmatrix} 0 & 1 & -4 \\ 11 & -3 & 1 \\ -22 & 6 & -2 \end{bmatrix} \to \begin{bmatrix} 0 & 1 & -4 \\ 11 & -3 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$
$$\to \begin{bmatrix} 0 & 1 & 0 \\ 11 & -3 & -11 \\ 0 & 0 & 0 \end{bmatrix} \to \begin{bmatrix} 0 & 1 & 0 \\ 0 & -3 & -11 \\ 0 & 0 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 \\ 0 & 11 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

d) Let $A = \left[\begin{smallmatrix} 3 & 1 \\ -1 & 2 \end{smallmatrix}\right]$ as in part (a). We can regart A as a module homomorphism $V \to L$, so by diagonalizing A we can find (lattice) bases (v_1, v_2) for V and (l_1, l_2) for L such that $l_1 = v_1$ and $l_2 = 7v_2$. We could do this systematically by keeping track of what each row and column operation does to each basis, but as is the case with most of these problems, it's simply easier to draw a picture and find such bases by hand. We find that $v_1 = (1, 2)$ and $v_2 = (1, 1)$ is a basis for V (note that $\det \left[\begin{smallmatrix} 1 & 2 \\ 1 & 1 \end{smallmatrix}\right] = -1$), and that $l_1 = v_1$ and $l_2 = 7v_2$ is a basis for L.

Joe Rabinoff