Kris Harper
MATH 25800

Homework 4

February 15, 2010

Problem 1 (9.4.2)**.** *Prove that the following polynomials are irreducible in* $\mathbb{Z}[x]$*:*
(a) $x^4 - 4x^3 + 6$
(c) $x^4 + 4x^3 + 6x^2 + 2x + 1$*.*

Proof. (a) This follows from Eisenstein's Criterion since $2 \mid -4$ and $2 \mid 6$ but $4 \nmid 6$.

(c) Substituting $x - 1$ for x gives the polynomial $x^4 - 2x + 2$, which is irreducible in $\mathbb{Z}[x]$ by Eisenstein's Criterion since $2 \mid 2$ but $4 \nmid 2$. But this means the original polynomial must also be irreducible in $\mathbb{Z}[x]$ since any factorization of it would give a factorization of $x^4 - 2x + 2$ by substituting $x - 1$. □

Problem 2 (9.4.5)**.** *Find all the monic irreducible polynomials of degree* ≤ 3 *in* $\mathbb{F}_2[x]$*, and the same in* $\mathbb{F}_3[x]$*.*

Proof. Note that since we're only interested in polynomials of degree less than or equal to 3, they will only be reducible in $\mathbb{F}_2[x]$ if they have a root in $\mathbb{F}_2$.

First consider degree three polynomials of the form $p(x) = x^3 + ax^2 + bx + c$. Since $p(0) = c$, if $c = 0$, then $p(x)$ has a root. Therefore $c = 1$. Also $p(1) = 1 + a + b + 1 = a + b$ so we need $a + b \neq 0$. Thus, either $a = 1$ and $b = 0$ or $b = 1$ and $a = 0$. Therefore the only possibilities for $p(x)$ are $p(x) = x^3 + x^2 + 1$ and $p(x) = x^3 + x + 1$.

Now suppose $p(x) = x^2 + ax + b$. We immediately see that $b = 1$ as before. Since $p(1) = 1 + a + 1 = a$, we also have $a = 1$ so the only choice is $p(x) = x^2 + x + 1$. Finally, $p(x) = x + 1$ is an irreducible polynomial in $\mathbb{F}_2[x]$.

Now suppose we're working in $\mathbb{F}_3[x]$. We have $p(x) = x^3 + ax^2 + bx + c$ and we have right away that $c = 1$ or $c = 2$. If $c = 1$ then $p(1) = 1 + a + b + 1 = a + b + 2$ so $a + b \neq 1$ and $p(2) = 2 + a + 2b + 1 = a + 2b$ so $a + 2b \neq 0$. This gives $a = 0$ and $b = 2$, $a = 1$ and $b = 2$, $a = 2$ and $b = 1$ or $a = 2$ and $b = 0$. Otherwise if $c = 2$ then $p(1) = 1 + a + b + 2 = a + b$ so $a + b \neq 0$ and $p(2) = 2 + a + 2b + 2 = a + 2b + 1$ so $a + 2b + 1 \neq 0$. This gives $a = 0$ and $b = 2$, $a = 1$ and $b = 0$, $a = 1$ and $b = 1$ or $a = 2$ and $b = 2$. So the possible polynomials are $p(x) = x^3 + 2x + 1$, $p(x) = x^3 + x^2 + 2x + 1$, $p(x) = x^3 + 2x^2 + x + 1$, $p(x) = x^3 + 2x^2 + 1$, $p(x) = x^3 + 2x + 2$, $p(x) = x^3 + x^2 + 2$, $p(x) = x^3 + x^2 + x + 2$ and $p(x) = x^3 + 2x^2 + 2x + 2$.

Consider $p(x) = x^2 + ax + b$ in $\mathbb{F}_3[x]$. We see that $b = 1$ or $b = 2$. If $b = 1$ then $p(1) = 1 + a + 1 = a + 2$ so $a \neq 1$. Also $p(2) = 1 + 2a + 1 = 2a + 2$ so $a \neq 2$. Therefore the only choice is $a = 0$. Similarly if $b = 2$ then $p(1) = 1 + a + 2 = a$ so $a \neq 0$ and $p(2) = 1 + 2a + 2 = 2a$ so $a \neq 0$. Thus the possible choices are $p(x) = x^2 + 1$, $p(x) = x^2 + x + 2$ and $p(x) = x^2 + 2x + 2$.

Finally note that the polynomials $x + 1$, $x + 2$, $2x + 1$ and $2x + 2$ are irreducible in $\mathbb{F}_3[x]$. □

Problem 3 (9.4.6)**.** *Construct fields of each of the following orders: (a)* 9*, (b)* 49*, (c)* 8*, (d)* 81 *(you may exhibit these as* $F[x]/(f(x))$ *for some* F *and* f*).*

Proof. (a) We know that if F is a field with order q and $f(x)$ is an irreducible polynomial of degree n, then $F[x]/(f(x))$ is a field with q^n elements. So we need an irreducible polynomial of degree 2 over the field $\mathbb{F}_3$. Using Problem 2 we see that $f(x) = x^2 + 1$ will work. Then $\mathbb{F}_3[x]/(x^2 + 1)$ is a finite field with $3^2 = 9$ elements.

(b) As in part (a) we need a degree 2 polynomial over $\mathbb{F}_7$ which is irreducible. Let $p(x) = x^2 + 1$ and note that $p(0) = 1$, $p(1) = 2$, $p(2) = 5$, $p(3) = 3$, $p(4) = 3$, $p(5) = 5$ and $p(6) = 2$. Thus $p(x)$ has no root in $\mathbb{F}_7$ and since it's degree 2, this means it's irreducible. Therefore $\mathbb{F}_7/(x^2 + 1)$ is a field with $7^2 = 49$ elements.

(c) We wish to find an irreducible polynomial of degree 3 over $\mathbb{F}_2$. Using Problem 2 again we see that $x^3 + x + 1$ will work. Now $\mathbb{F}_2/(x^3 + x + 1)$ is a field with $2^3 = 8$ elements.

(d) We wish to find an irreducible polynomial of degree 2 in $(\mathbb{F}_3/(x^2 + 1))[y]$. Choose $p(y) = y^2 + y + 2$. Note that if $p(y) = 0$ then $y^2 + y + 2 = \overline{x^2 + 1} = \overline{x}^2 + 1$ so $y^2 + y + 1 = \overline{x}^2$. It's now clear that $p(\overline{0}) \neq 0$, $p(\overline{1}) \neq 0$, $p(\overline{2}) \neq 0$, $p(\overline{x}) \neq 0$ and $p(\overline{2x}) \neq 0$. Note also that $p(\overline{x+1}) = \overline{x^2} \neq 0$, $p(\overline{x+2}) = \overline{x^2 + 2x} \neq 0$, $p(\overline{2x+1}) = \overline{x^2} \neq 0$ and $p(\overline{2x+2}) = \overline{x^2 + x} \neq 0$. Therefore $p(y)$ has no roots and is a degree 2 polynomial. It is thus irreducible and $(\mathbb{F}_3/(x^2 + 1))[y]/(y^2 + y + 2)$ is a field with $9^2 = 81$ elements. □

Problem 4 (9.4.7)**.** *Prove that* $\mathbb{R}[x]/(x^2 + 1)$ *is a field which is isomorphic to the complex numbers.*

Proof. It follows immediately that $\mathbb{R}[x]/(x^2+1)$ is field since (x^2+1) is irreducible in $\mathbb{R}[x]$ (it has no root and is of degree 2). Let $\varphi : \mathbb{R}[x] \to \mathbb{C}$ be given by $\varphi(p(x)) = p(i)$, that is, evaluation at i. This is a ring homomorphism since evaluation maps are ring homomorphisms. It's also surjective since given $a+bi \in \mathbb{C}$, the polynomial $a+bx \in \mathbb{R}[x]$ is mapped to it. Also note that $\varphi(x^2+1) = 0$ and so $(x^2+1) \subseteq \ker\varphi$. For $p(x) \in \ker\varphi$, we have $p(i) = 0$. Since $\mathbb{R}[x]$ is a U.F.D, we must have some factor $(x^2+1) \mid p(x)$ so $p(x) \in (x^2+1)$. Thus $\ker\varphi \subseteq (x^2+1)$ and $\ker\varphi = (x^2+1)$. Now from the First Isomorphism Theorem we have $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$. □

Problem 5 (9.4.14)**.** *Factor each of the two polynomials: x^8-1 and x^6-1 into irreducibles over each of the following rings: (a) $\mathbb{Z}$, (b) $\mathbb{Z}/2\mathbb{Z}$, (c) $\mathbb{Z}/3\mathbb{Z}$.*

Proof. (a) $x^8-1 = (x^4+1)(x^2+1)(x+1)(x-1)$ and $x^6-1 = (x^2+x+1)(x^2+x-1)(x+1)(x-1)$.
(b) $x^8-1 = (x+1)^8$ and $x^6-1 = (x+1)^2(x^2+x+1)^2$.
(c) $x^8-1 = (x^2+2x+2)(x^2+x+2)(x^2+1)(x+2)(x+1)$ and $x^6-1 = (x+2)^3(x+1)^3$. □

Problem 6 (9.4.19)**.** *Let F be a field and let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 \in F[x]$. The* derivative*, $D_x(f(x))$, of $f(x)$ is defined by*

$$D_x(f(x)) = na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$$

where, as usual, $na = a + a + \cdots + a$ (n times). Note that $D_x(f(x))$ is again a polynomial with coefficients in F.

The polynomial $f(x)$ is said to have a multiple root *if there is some field E containing F and some $\alpha \in E$ such that $(x-\alpha)^2$ divides $f(x)$ in $E[x]$. For example, the polynomial $f(x) = (x-1)^2(x_2) \in \mathbb{Q}[x]$ has $\alpha = 1$ as a multiple root and the polynomial $f(x) = x^4+2x^2+1 = (x^2+1)^2 \in \mathbb{R}[x]$ has $\alpha = \pm i \in \mathbb{C}$ as multiple roots. We shall prove in Section 13.5 that a nonconstant polynomial $f(x)$ has a multiple root if and only if $f(x)$ is not relatively prime to its derivative (which can be detected by the Euclidean Algorithm in $F[x]$). Use the criterion to determine whether the following polynomials have multiple roots:*
(a) $x^3-3x-2 \in \mathbb{Q}[x]$
(b) $x^3+3x+2 \in \mathbb{Q}[x]$
(c) $x^6-4x^4+6x^3+4x^2-12x+9 \in \mathbb{Q}[x]$
(d) Show that for any prime p and any $a \in \mathbb{F}_p$ that the polynomial x^p-a has a multiple root.

Proof. (a) The derivative of this polynomial is $3x^2-3$ and these two polynomials share a common factor of $x+1$ so they're not relatively prime. The original polynomial therefore has no multiple roots.

(b) The derivative of this polynomial is $3x^2+3$ and these two polynomials are relatively prime so the original must have a multiple root.

(c) The derivative of this polynomial is $6x^5-16x^3+18x^2+8x-12$ and these two polynomials share a common factor of x^3-2x+3 so they're not relatively prime. The original polynomial therefore has no multiple roots.

(d) The derivative of x^p-a is px^{p-1}. But in $\mathbb{F}_p$, $p=0$ so the derivative is 0. Therefore these two polynomials are not relatively prime and x^p-a has no multiple roots. □

Problem 7 (9.4.20)**.** *(a) Show that the reduction of $f(x)$ modulo both of the nontrivial ideals* (2) *and* (3) *of $\mathbb{Z}/6\mathbb{Z}[x]$ is an irreducible polynomial, showing that the condition that R be an integral domain in Proposition 12 is necessary.*

Proof. (a) Note that $(\mathbb{Z}/6\mathbb{Z})/(2) \cong \mathbb{Z}/2\mathbb{Z}$ and $(\mathbb{Z}/6\mathbb{Z})/(3) \cong \mathbb{Z}/3\mathbb{Z}$. It's clear that x is not reducible over either of these rings. □

Problem 8 (9.5.2)**.** *For each of the fields constructed in Exercise 6 of Section 4 exhibit a generator for the (cyclic) multiplicative group of nonzero elements.*

Kris Harper
MATH 25800
Homework 4
February 15, 2010

Proof. (a) We wish to find an element of $\mathbb{F}_3[x]/(x^2+1)$ which has order 8. Consider the element $\overline{x+1}$. Note that $|(\mathbb{F}_3[x]/(x^2+1))^\times| = 8$ so we only need to check that $\overline{x+1}^2 \neq 1$ and $\overline{x+1}^4 \neq 1$. But $\overline{x+1}^2 = \overline{x^2+2x+1} = \overline{2x}$ and $\overline{x+1}^4 = \overline{x^4+4x^3+6x^2+4x+1} = \overline{2}$ using the division algorithm. Thus $|\overline{x+1}| = 8$ and this is a generator for the group.

(b) This group has order 48 so it suffices to check that an element is not 1 when raised to the 24^{th} power. Using the division algorithm, we see that $\overline{x+2}^2 4 = \overline{6}$ so $\overline{x+2}$ is a generator for this set.

(c) This group has order 7 which is prime. It thus suffices to find a nonzero, nonidentity element. Choose $\overline{x+1}$.

(d) We need to find an element which when raised to the 40^{th} power is not the identity. Note that from part (a), $\overline{x+1}$ is an element of the underlying field $\mathbb{F}_3[x]/(x^2+1)$ which has order 8. Choose this as a coefficient for $\overline{y+1}$ to get $\overline{\overline{x+1}(y+1)}$. This polynomial is not the identity when raised to the 40^{th} power and so must be a generator for the multiplicative group of our finite field. □

Problem 9 (9.5.5)**.** *Let φ denote Euler's φ-function. Prove the identity $\sum_{d|n} \varphi(d) = n$, where the sum is extended over all the divisors d of n.*

Proof. Let A be a cyclic group of order n. Let $d \mid n$ and note that A contains a unique subgroup of order d. Note that the number of generators of Z_d is simply $\varphi(d)$ since this is the number of elements which are relatively prime to d. Therefore there are $\varphi(d)$ generators for each subgroup of order d and each of these generators must have order d (since Z_d is cyclic). Now, since order is unique to each element, we can use Lagrange's Theorem and sum over all possible divisors $d \mid n$ to $\sum_{d|n} \varphi(d) = n$. □

Problem 10 (10.1.3)**.** *Assume that $rm = 0$ for some $r \in R$ and some $m \in M$ with $m \neq 0$. Prove that r does not have a left inverse (i.e., there is no $s \in R$ such that $sr = 1$).*

Proof. We know that $1m = 1$ and $s0 = 0$ for all $m \in M$ and $s \in R$. Then multiplying on the left by such an s would give $m = 1m = (sr)m = s(rm) = s0 = 0$ and we've assumed $m \neq 0$. Thus such an s cannot exist. □

Problem 11 (10.1.4)**.** *Let M be the module R^n described in Example 3 and let $I_1, I_2, \ldots, I_n$ be left ideals of R. Prove that the following are submodules of M:*
(a) $\{(x_1, x_2, \ldots, x_n) \mid x_i \in I\}$
(b) $\{(x_1, x_2, \ldots, x_n) \mid x_i \in R$ and $x_1 + x_2 + \cdots + x_n = 0\}$.

Proof. (a) Let N be the set in question. We see that $N \neq \emptyset$ since each $I_i \neq \emptyset$. Let $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in N$ and let $r \in R$. Then

$$(x_1, \ldots, x_n) + r(y_1, \ldots, y_n) = (x_1 + ry_1 + \cdots + x_n + ry_n).$$

Since I_i is a left ideal, $ry_i \in I_i$. Furthermore, since ideals are subgroups of R, $x_i + ry_i \in I_i$. Therefore, this element is an element of N so N fits the submodule criterion and is a submodule of M.

(b) Let N be the set in question as before. Once again, N isn't empty since $0 \in I_i$ for each i so $(0, \ldots, 0) \in N$. Let $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in N$ and let $r \in R$. Then

$$(x_1, \ldots, x_n) + r(y_1, \ldots, y_n) = (x_1 + ry_1 + \cdots + x_n + ry_n).$$

Note that each coordinate is an element of I_i as in part (a). Furthermore,

$$\sum_{i=1}^{n}(x_i + ry_i) = \sum_{i=1}^{n} x_i + \sum_{i=1}^{n} ry_i = \sum_{i=1}^{n} x_i + r\sum_{i=1}^{n} y_i = 0 + r0 = 0.$$

Therefore, this element is in N and N fits the submodule criterion so N is a submodule of M. □

Kris Harper
MATH 25800
Homework 4 February 15, 2010

Problem 12 (10.1.7)**.** *Let $N_1 \subseteq N_2 \subseteq \dots$ be an ascending chain of submodules of M. Prove that $\bigcup_{i=1}^{\infty} N_i$ is a submodule of N.*

Proof. Let A be the set in question. Since $N_1 \subseteq A$, we see that $A \neq \emptyset$. Suppose $x, y \in A$ and let $r \in R$. Then $y \in N_i$ for some i and thus $ry \in N_i$ as well since N_i is a submodule. But then $ry \in A$ as well. Likewise, $x \in N_j$ for some j. Without loss of generality, let $i \leq j$ so that $ry \in N_j$ as well. But the $x + ry \in N_j$ and $x + ry \in A$. Therefore A is a submodule. □

Problem 13 (10.1.8)**.** *An element m of the R-module M is called a* torsion element *if $rm = 0$ for some nonzero element $r \in R$. The set of torsion elements is defined*

$$\mathrm{Tor}(M) = \{m \in M \mid rm = 0 \text{ for some nonzero } r \in R\}.$$

(a) Prove that if R is an integral domain then $\mathrm{Tor}(M)$ is a submodule of M (called the torsion *submodule of M).*
(b) Give an example of a ring R and an R-module M such that $\mathrm{Tor}(M)$ is not a submodule. (c) If R has zero divisors show that every nonzero R-module has nonzero torsion elements.

Proof. (a) Suppose R is an integral domain. Note that $0 \in \mathrm{Tor}(M)$ so $\mathrm{Tor}(M) \neq \emptyset$. Let $x, y \in \mathrm{Tor}(M)$ and $a, b, r \in R$ such that $ax = by = 0$ with a and b nonzero. Then $ab(x + y) = 0$ and $a(rx) = (ar)x = 0$ so $\mathrm{Tor}(M)$ is a submodule of M.

(b) Let $R = \mathbb{Z}/6\mathbb{R}$ and $M = R$. Then $2, 3 \in \mathrm{Tor}(M)$ since $2 \cdot 3 = 0$ but $2 \neq 0$ and $3 \neq 0$. But then $2 + 3 = 5$ and $5 \notin \mathrm{Tor}(M)$. Thus $\mathrm{Tor}(M)$ is not a submodule.

(c) Let $m \in M$ and let $x, y \in R$ such that x and y are nonzero but $xy = 0$. Then $ym \in \mathrm{Tor}(M)$ since $x(ym) = (xy)m = 0m = 0$. □

Problem 14 (10.1.14)**.** *Let z be an element of the center of R, i.e., $zr = rz$ for all $r \in R$. Prove that zM is a submodule of M, where $zM = \{zm \mid m \in M\}$. Show that if R is the ring of 2×2 matrices over a field and e is the matrix with a 1 in position $1, 1$ and zeros elsewhere then eR is* not *a left R-submodule (where $M = R$ is considered as a left R-module as in Example 1) — in this case the matrix e is not in the center of R.*

Proof. Note that $zM \neq \emptyset$ since $0 \in zM$. Let $zx, zy \in zM$ and let $r \in R$. Then $zx+rzy = zx+zry = z(x+ry)$ so this is an element of zM as well and zM is a submodule of M. Now let R be the ring of matrices defined above with e defined as above as well. Note that a matrix in eR will have two possibly nonzero elements in the first row, and two zero elements in the second row. But these matrices are clearly not closed under multiplication by elements of R. For example, multiplying by the matrix with all 1s as entries puts the upper left coordinate in the lower left coordinate. This is not an element of eR so eR is not an R-submodule. □

Problem 15 (10.1.22)**.** *Suppose that A is a ring with identity 1_A that is a (unital) left R-module satisfying $r \cdot (ab) = (r \cdot a)b = a(r \cdot b)$ for all $r \in R$ and $a, b \in A$. Prove that the map $f : R \to A$ defined by $f(r) = r \cdot 1_A$ is a ring homomorphism mapping 1_R to 1_A and that $f(R)$ is contained in the center of A. Conclude that A is an R-algebra and that the R-module structure on A induced by its algebraic structure is precisely the original R-module structure.*

Proof. Let $r, s \in R$. Note that

$$f(r+s) = (r+s)\cdot 1_A = 1_A((r+s)\cdot 1_A) = 1_A(r\cdot 1_A + s\cdot 1_A) = 1_A(r\cdot 1_A) + 1_A(s\cdot 1_A) = r\cdot 1_A + s\cdot 1_A = f(r)+f(s).$$

Likewise

$$f(rs) = (rs) \cdot 1_A = 1_A((rs) \cdot 1_A) = 1_A(r \cdot (s \cdot 1_A)) = (r \cdot 1_A)(s \cdot 1_A) = f(r)f(s).$$

We also have $f(1_R) = 1_R \cdot 1_A = 1_A$. Now let $f(r) \in f(R)$ so that $f(r) = r \cdot 1_A$ and let $a \in A$. Then

$$f(r)a = (r \cdot 1_A)a = r \cdot (1_A a) = r \cdot (a1_A) = a(r \cdot 1_A) = af(r)$$

so $f(r)$ is in the center of A and $f(R)$ is a subset of the center of A. This shows that A is an R-algebra. When viewed as an R-module, this R-algebra is precisely the same as if we view A itself as an R-module. □

Kris Harper
MATH 25800
Homework 4 February 15, 2010

Problem 16 (10.2.4)**.** *Let A be an $\mathbb{Z}$-module, let a be any element of A and let n be a positive integer. prove that the map $\varphi_a : \mathbb{Z}/n\mathbb{Z} \to A$ given by $\varphi_a(\overline{k}) = ka$ is a well defined $\mathbb{Z}$-module homomorphism if and only if $na = 0$. Prove that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \cong A_n$, where $A_n = \{a \in A \mid na = 0\}$ (so A_n is the annihilator in A of the ideal (n) of $\mathbb{Z}$—cf. Exercise 10, Section 1).*

Proof. First we show that φ_a is a homomorphism. Let $\overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z}$ and let $m \in \mathbb{Z}$. Then

$$\varphi_a(\overline{x} + \overline{y}) = \varphi_a(\overline{x+y}) = (x+y)a = xa + ya = \varphi_a(\overline{x}) + \varphi_a(\overline{y})$$

and

$$\varphi_a(m\overline{x}) = (mx)a = m(xa) = m\varphi_a(\overline{x}).$$

Now suppose φ_a is well defined. Then consider

$$0 = 0 \cdot a = \varphi_a(\overline{0}) = \varphi_a(\overline{n-1} + \overline{1}) = \varphi_a(\overline{n-1}) + \varphi_a(\overline{1}) = (n-1)a + a = na$$

so $na = 0$. Conversely, suppose that $na = 0$. Let $\overline{x} = \overline{y}$. Write $x = x' + cn$ and $y = y' + dn$ where $0 \leq x' \leq n-1$ and $0 \leq y' \leq n-1$. Then since $\overline{x} = \overline{y}$, we must have $x' = y'$ so that

$$\varphi_a(\overline{x}) = xa = (x' + cn)a = x'a + cna = x'a = y'a = y'a + dna = (y' + dn)a = ya = \varphi_a(\overline{y}).$$

Thus φ_a is well-defined. Let $\psi : \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \to A_n$ be defined by $\psi(\varphi) = \varphi(\overline{1})$. Note that

$$\psi(\varphi_1 + \varphi_2) = (\varphi_1 + \varphi_2)(\overline{1}) = \varphi_1(\overline{1}) + \varphi_2(\overline{1}) = \psi(\varphi_1 + \varphi_2)$$

and for $m \in \mathbb{Z}$

$$\psi(m\varphi) = (m\varphi)(\overline{1}) = m(\varphi(\overline{1})) = m\psi(\varphi)$$

so ψ is a module homomorphism. We've shown that ψ is surjective since the homomorphisms φ_a are each mapped to $a \in A_n$. Furthermore, if $\varphi_1(\overline{1}) = \varphi_2(\overline{1})$ then it follows that $\varphi_1(\overline{k}) = \varphi_2(\overline{k})$ because this is simply $\varphi_i(\overline{1})$ added to itself k times. Thus $\varphi_1 = \varphi_2$ and ψ is injective. Thus $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \cong A_n$. □

Problem 17 (10.2.7)**.** *Let z be a fixed element of the center of R. Prove that the map $m \mapsto zm$ is an R-module homomorphism from M to itself. Show that for a commutative ring R the map from R to $\mathrm{End}_R(M)$ given by $r \mapsto rI$ is a ring homomorphism (where I is the identity endomorphism).*

Proof. Let $m, n \in M$ and $r \in R$. Then we have $z(m+n) = zm + zn$ and $z(rm) = (zr)m = (rz)m = r(zm)$ so the map is both additive and scalar multiplicative and is thus a module homomorphism. Now suppose $\varphi : R \to \mathrm{End}_R(M)$ and let $r, s \in R$. Then $\varphi(r+s) = (r+s)I = rI + sI = \varphi(r) + \varphi(s)$ and $\varphi(rs) = (rs)I = (rI)(sI) = \varphi(r)\varphi(s)$. Note that we need R to be commutative to ensure that each rI is actually an R-module homomorphism from M to itself (since now the center of R is all of R). □

Problem 18 (10.2.8)**.** *Let $\varphi : M \to N$ be an R-module homomorphism. Prove that $\varphi(\mathrm{Tor}(M)) \subseteq \mathrm{Tor}(N)$ (cf. Exercise 8 in Section 1).*

Proof. Let $m \in \mathrm{Tor}(M)$ such that $rm = 0$ for $r \neq 0$. Then since φ is an R-module homomorphism we have $r\varphi(m) = \varphi(rm) = \varphi(0) = 0$ in N. Thus $\varphi(r) \in \mathrm{Tor}(N)$ and $\varphi(\mathrm{Tor}(M)) \subseteq \mathrm{Tor}(N)$. □