Solutions for Tutorial 7 – Algebra 2019

(1) Let R be an integral domain, and let a and b be elements of R.

(a) Show that $a = bc$ implies $(a) \subseteq (b)$ with equality if and only if c is a unit.

Assume we have $a = bc$, and let ra be an element of (a), where $r \in R$ is arbitrary. Then we have $ra = rcb \in (b)$. This proves the inclusion. If c is a unit, then apply the same argument to $b = ac^{-1}$ to obtain the other inclusion. If we have equality, then we have $b \in (b) = (a)$, so there exists an element $d \in R$ with $b = da$. Further

$$1 \cdot a = a = cb = cda,$$

so

$$(1 - cd)a = 0.$$

Since R is an integral domain, we have either $a = 0$, in which case the statement you were supposed to prove is false, I was careless here, or we have $cd = 1$, and hence c is a unit.

(b) Show that $(a) = (b)$ if and only if there exists a unit $u \in R^\times$ with $a = ub$.

Let us first look at the case $(a) = (b) = \{0\}$, since that was iffy in the last part. This is the case if and only if we have $a = b = 0$, and we can take $u = 1$. So, assume now that $(a) = (b)$ where a and b are non-zero elements of R. The "if" statement is then answered in the previous question. To see the "only if" part, note that $a \in (a) = (b)$ implies the existence of $c \in R$ with $a = cb$ and use the previous question to deduce that c is a unit.

(c) Let $u \in R^\times$ be a unit. Show that $(u) = R$.

For any $r \in R$, we have $r = ru^{-1}u \in (u)$.

(2) Prove that a $\mathbb{Z}$-module consists of the same data as an abelian group.

By defnintion, a $\mathbb{Z}$-module is an abelian group M together with a bilinear map

$$\begin{array}{rcl} \mathbb{Z} \times M & \longrightarrow & M \\ (z, m) & \longmapsto & zm \end{array}$$

(multiplication by scalars) satisfying $1m = m$ and $z_1(z_2 m) = (z_1 z_2)m$. Given a $\mathbb{Z}$-module, we may therefore forget the multiplication by scalars and just remember that M is an abelian group.

On the other hand, assume an abelian group A is given. We need to show that there is one and only one way to equip A with the structure of a $\mathbb{Z}$-module in such a manner that the underlying abelian group is the original one. Indeed, as in any module we must have $1a = a$ and $0a = 0$. Distributivity then forces $za = \underbrace{a + \cdots + a}_{z \text{ times}}$ for $z \in \mathbb{Z}$ positive and further $za = (-z)(-a)$ for negative z.

One checks that this scalar multiplication makes A into a $\mathbb{Z}$-module. Moreover, all the constructions above are "functorial" meaning that they also translate between $\mathbb{Z}$-module homomorphisms and homomorphisms of abelian groups.

An alternative proof uses a reformulation of the definition of module: let M be an abelian group, let R be a ring, and write $End(M)$ for the endomorphism ring of M. (Recall that an endomorphism of M is just a group homomorphism from M to M.) Then a scalar multiplication of R on M (i.e., an R-module structure on M whose underlying abelian group is the given one) is given by the same data as a ring homomorphism from R to $End(M)$. Try to prove this – it should remind you of the analogous statement for group actions and bijections.

The statement about $\mathbb{Z}$-modules amounts then to the fact we saw in class that every ring, so in particular $End(A)$, receives exactly one ring homomorphism from $\mathbb{Z}$.

(3) Consider the abelian group A with generators a, b and c and relations $3a = b - c$, $6a = 2c$ and $3b = 4c$.

(a) Write A as the quotient of a free $\mathbb{Z}$-module by a submodule.

$$A = \mathbb{Z}\{a, b, c\}/\langle 3a - b + c, 6a - 2c, 3b - 4c\rangle.$$

(b) Convince yourself that A is isomorphic to the cyclic group on twelve elements.

The generator b is superfluous, $b = 3a + c$. So,

$$A = \langle a, c \mid 6a - 2c = 0, 9a - c = 0\rangle.$$

Similarly, we can eliminate the generator $c = 9a$ and arrive at

$$A = \langle a \mid -12a = 0\rangle \cong \mathbb{Z}/12\mathbb{Z}.$$

(c) Use the language of generators and relations to give a map f from A to $\mathbb{Z}/12\mathbb{Z}$ and an inverse of f.

We claim that

$$\begin{aligned} f : A &\longrightarrow \mathbb{Z}/12\mathbb{Z} \\ a &\longmapsto 11 \\ b &\longmapsto 0 \\ c &\longmapsto 3 \end{aligned}$$

is a well defined group homomorphism. Indeed, the relations hold in the image:

$$\begin{aligned} 3f(a) = 9 &= 0 - 3 = f(b) - f(c) \\ 6f(a) = 6 &= 2f(c) \\ 3f(b) = 0 &= 4 \cdot 3 = 4f(c). \end{aligned}$$

We claim that f is an isomorphism with inverse

$$\begin{aligned} g : \mathbb{Z}/12\mathbb{Z} &\longrightarrow A \\ 1 &\longmapsto -a. \end{aligned}$$

First, g is well defined, because $-a$ has order 12 in A. Next, $f(-a) = -f(a) = 1$, so we have $f \circ g = id$. We already know that both groups have 12 elements, so we are done, but let us pretend we don't know this. Then need to use the relations in A to prove the equations

$$\begin{aligned} g(f(a)) = g(11) &= -g(1) = -(-a) = a \\ g(f(b)) = g(0) &= 0 = b \\ g(f(c)) = g(3) &= -3a = c \end{aligned}$$

and obtain $gf = id$.

(d) Now translate this into the language of universal properties.

To define the map $f : A \longrightarrow \mathbb{Z}/12\mathbb{Z}$, we first use the universal property of free $\mathbb{Z}$-module to define a map

$$\begin{array}{ccccccc} \widetilde{f} : \mathbb{Z}\{a,b,c\} & \dashrightarrow & \mathbb{Z}/12\mathbb{Z} & & 11 & 0 & 3 \\ \uparrow & \nearrow & & \nearrow & \nearrow & \nearrow & \\ \{a,b,c\} & & & a & b & c & \end{array}$$

$$a \mapsto 11, \quad b \mapsto 0, \quad c \mapsto 3$$

and then check that

$$\begin{aligned} \widetilde{f}(3a - b + c) &= 0 \\ \widetilde{f}(6a - 2c) &= 0 \\ \widetilde{f}(3b - 4c) &= 0. \end{aligned}$$

Hence $\widetilde{f}$ vanishes on the submodule generated by these three elements

$$\langle 3a - b + c, 6a - 2c, 3b - 4c \rangle$$

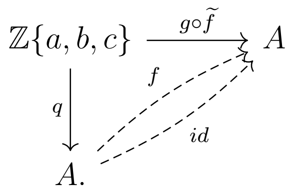
and the universal property of quotient modules gives our map f as follows

$$\begin{array}{ccc} \mathbb{Z}\{a,b,c\} & \xrightarrow{\widetilde{f}} & \mathbb{Z}/12\mathbb{Z} \\ {\scriptstyle q}\downarrow & \overset{f}{\nearrow} & \\ A. & & \end{array}$$

Similarly, we obtain the map g,

$$\begin{array}{ccc} 1 & \longmapsto & -a \\ \mathbb{Z} & \xrightarrow{\widetilde{g}} & A \\ {\scriptstyle q'}\downarrow & \overset{g}{\nearrow} & \\ \mathbb{Z}/12\mathbb{Z}. & & \end{array}$$

To show that $g \circ f$ is the identity of A, we check, argue that $g \circ \widetilde{f} = q$ (this boils down to using the relations in A) and conclude, using the uniqueness of the universal property for q that $g \circ f = id_A$,



The argument for $fg = id$ is similar.

(4) Consider the field $\mathbb{F}_8$. To be concrete, use the construction and notation from class, so $\mathbb{F}_8$ is generated over $\mathbb{F}_2$ by an element b satisfying the relation $b^3 = b+1$. Consider the element $b^2 \in \mathbb{F}_8$.

(a) Without any calculations, determine the degree of b^2 over $\mathbb{F}_2$.

(b) Prove your statement from (a).

We have

$$3 = deg_{\mathbb{F}_2}(b^2) \cdot deg_{\mathbb{F}_2(b^2)}\mathbb{F}_8,$$

so the degree must be either 1 or 3. Since b^2 is not an element of $\mathbb{F}_2$, its degree must be 3.

(c) Find the irreducible polynomial of b^2 over $\mathbb{F}_2$.

We are looking for a polynomial of degree three vanishing on b^2. We have

$$(b^2)^3 = (b^3)^2 = (b+1)^2 = b^2 + 1,$$

so, the irreducible polynomial of b^2 equals $p(x) = x^3 + x + 1$.

(d) Write down an automorphism of $\mathbb{F}_8$.

Since b and b^2 have identical irreducible polynomial, we have the field homomorphism

$$\begin{array}{rcl} \mathbb{F}_8 & \longrightarrow & \mathbb{F}_8 \\ b & \longmapsto & b^2, \end{array}$$

which is automatically an isomorphism for cardinality reasons.