7210 HW 7

Duncan Wilkie

25 October 2022

Problem 1 (D&F 7.1.30). *Let $A = \mathbb{Z} \times \mathbb{Z} \times \cdots$ be the direct product of copies of $\mathbb{Z}$ indexed by the positive integers (so A is a ring under componentwise addition and multiplication) and let R be the ring of all group homomorphisms from A to itself with addition pointwise and multiplication defined as function composition. Let ϕ be the element of R defined by $\phi(a_1, a_2, a_3, ...) = (a_2, a_3, ...)$. Let ψ be the element of R defined by $\psi(a_1, a_2, a_3, ...) = (0, a_1, a_2, a_3, ...)$*

1. *Prove that $\phi\psi$ is the identity of R but $\psi\phi$ is not the identity of R (i.e. ψ is a right, but not a left, inverse for ϕ).*
2. *Exhibit infinitely many right inverses for ϕ.*
3. *Find a nonzero element π in R such that $\phi\pi = 0$ but $\pi\phi \neq 0$.*
4. *Prove that there is no nonzero element $\lambda \in R$ such that $\lambda\phi = 0$ (i.e. ϕ is a left zero divisor but not a right zero divisor).*

Solution. $\phi \circ \psi(a_1, a_2, \cdots) = \phi(0, a_1, a_2, \cdots) = (a_1, a_2, \cdots)$; since $(a_1, a_2, \cdots)$ is a general element of A, q this proves $\phi \circ \psi$ is the identity function id_A, which is the ring identity on R, since $id_A \circ f = f \circ id_A = f$ for all (set) endomorphisms f on A. Inversely, $\psi \circ \phi(a_1, a_2, a_3, \cdots) = \psi(a_2, a_3, \cdots) = (0, a_2, a_3, \cdots)$, and taking any element of A with $a_1 \neq 0$ shows $\psi\phi$ is not the identity.

Consider functions $f_i : (a_1, a_2, \cdots) \mapsto (i, a_1, a_2, \cdots)$; these are infinitely many right inverses to ϕ, since $\phi \circ f_i(a_1, a_2, \cdots) = \phi(i, a_1, a_2, \cdots) = (a_1, a_2, \cdots)$.

Taking $\pi : (a_1, a_2, \cdots) \mapsto (1, 0, \cdots)$, $\phi \circ \pi = \phi(1, 0, \cdots) = (0, 0, \cdots) = 0$ and $\pi \circ \phi = (1, 0, \cdots) \neq 0$.

Suppose $\lambda\phi(a_1, a_2, a_3 \cdots) = \lambda(a_2, a_3, \cdots) = 0$. If $\lambda \neq 0$, then there exists some input a such that $\lambda a \neq (0, 0, \cdots)$; the sequence $\psi(a)$ has $\lambda \circ \phi(\psi(a)) = \lambda(a) \neq 0$, showing $\lambda\phi \neq 0$. □

Problem 2 (D&F 7.3.29). *Let R be a commutative ring. Recall that an element $x \in R$ is nilpotent if $x^n = 0$ for some $n \in \mathbb{Z}^+$. Prove that the set of nilpotent elements from an ideal—called the nilradical of R and denoted $\eta(R)$.*

Solution. The set of nilpotent elements is first a subring. It contains the zero of the ring trivially, and if nonzero $a, b \in \eta(R)$ then $a^n = b^{n'} = 0$ for some $n, n' \in \eta(R)$, so assuming WLOG $n' \geq n$,

$$(a-b)^{nn'} = \sum_{k=0}^{nn'} \binom{nn'}{k} a^k (-b)^{nn'-k} = \sum_{k=0}^{n'} \binom{nn'}{k} a^k (-b)^{nn'-k} \sum_{k=n'}^{nn'} \binom{nn'}{k} a^k (-b)^{nn'-k}$$

$$= \sum_{k=0}^{n'} \binom{nn'}{k} a^k (-b)^{nn'-k} \sum_{k=n'}^{nn'} \binom{nn'}{k} a^{nn'-k} (-b)^{nn'}$$

In the left sum, every term has since $0 \le k \le n'$ and $n \ge 2$ (by a nonzero) that $nn' - k \ge n' \Leftrightarrow nn' \ge n' + k$, implying $b^{nn'-k} = 0$ and therefore also $(-b)^{nn'-k} = (-1)^{nn'-k} b^{nn'-k} = 0$, making the term and the whole sum zero. In the right sum, every term has since $n' \ge n$ that $a^k = 0$, making this sum also zero. Therefore, $(a-b)^{nn'} = 0$. If one of a, b are zero, then $a-b$ equals either 0, the other nonzero term, or the negative of the other nonzero term, all of which are immediately nilpotent, so for all $a, b \in \eta(R)$ one has $a - b \in \eta(R)$, i.e. R is closed under subtraction. Similarly, $(ab)^{nn'} = a^{nn'} b^{nn'}$ by commutativity (cf. proof of Lemma 6 of the first homework; it uses only associativity of group products), and since each exponent contains a factor of the element's nilpotency exponent, the term is zero.

Showing closure of the now-subring under multiplication is far easier: if $a \in \eta(R)$ has nilpotency exponent n and $r \in R$, then by commutativity $(ar)^n = a^n r^n = 0r^n = 0$, so $\eta(R)$ is a left-ideal and by commutativity also a right-sided ideal. □

Problem 3 (D&F 7.3.33)**.** *Assume R is commutative. Let $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ be an element of the polynomial ring $R[x]$.*

1. *Prove that $p(x)$ is a unit in $R[x]$ iff a_0 is a unit and $a_1, a_2, \ldots, a_n$ are nilpotent in R.*
2. *Prove that $p(x)$ is nilpotent in $R[x]$ iff $a_0, a_1, \ldots, a_n$ are nilpotent elements of R.*

Solution. Suppose a_0 is a unit and $a_1, a_2, \ldots, a_n$ are nilpotent with nilpotency exponents $k_1, k_2, \ldots, k_n$. First, note that $y = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x$ is nilpotent in $R[x]$: by commutativity, $(a_i x^i)^{k_i} = a_i^{k_i} x^{i+k_i} = 0x^{i+k_i} = 0$. The sum of nilpotent elements is again nilpotent by the above argument that $\eta(R)$ is an ideal and therefore closed under addition. Since a_0 is a unit in R, it's also a unit in $R[x]$, so $p(x)$ is the sum of a unit and a nilpotent element.

Conversely, suppose $p(x)$ is a unit. Then there exists $p^{-1}(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0$ such that $p(x)p^{-1}(x) = 1$; equivalently, the ith coefficient of the product polynomial is for all $i \ne 0$

$$\sum_{l=0}^{i} a_l b_{i-l} = 0$$

and for $i = 0$ $a_0 b_0 = 1$. Clearly, the latter shows that a_0 must be a unit. For nilpotency, we induct on the degree of polynomials in the formula "$p(x)$ is unit" $\Rightarrow$ "non-constant coefficients are nilpotent." It clearly holds for $\deg p = 0$ vacuously, since degree-zero polynomials have no non-constant coefficients. Presume it holds for all polynomials with degree less than n. One can additively cancel in the expression for the ith coefficient of the product to obtain

$$a_i b_0 = -\sum_{l=0}^{i-1} a_l b_{i-l}$$

Since b_0 is a unit with inverse a_0,

$$a_i = -a_0 \sum_{l=0}^{i-1} a_l b_{i-l}$$

The polynomial $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ has inverse $b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$, since in the product of p and p^{-1}, the nth terms of the factors only contribute to the nth term of the product, so omitting them merely removes that term. By the induction hypothesis, then $a_1, a_2 \ldots a_{n-1}$ are nilpotent. Similarly, $b_1, b_2, \ldots b_n$ are nilpotent, so every addend of the sum expression of a_n contains a nilpotent factor, and a_n is nilpotent. Accordingly, all non-constant coefficients of p are nilpotent, proving the converse.

For the second proposition, note that if $a_0, a_1, \ldots, a_n$ are nilpotent, the above argument that a_ix^i applies to show $p(x)$ is the sum of nilpotent elements and therefore nilpotent. Conversely, suppose $p(x)$ is nilpotent. We induct on the degree of p with the formula "$p(x)$ is nilpotent" $\Rightarrow$ "all its coefficients are nilpotent." The property once again holds for $\deg p = 0$ trivially; suppose it holds for $\deg p = n - 1$. Nilpotency to exponent k says

$$0 = (a_0 + a_1x + \cdots + a_nx^n)^k = \sum_{0 \le j_1 + j_2 + \cdots + j_n \le k} \binom{k}{j_1, j_2, \ldots, j_n} \prod_{l=1}^{n} a_l^{j_l} x^{l \cdot j_l},$$

using the multinomial theorem. The coefficient of x^{nk} in this sum is a_n^k: unless $j_n = k$, all other $j_i = 0$, and $l = n$ the product $l \cdot j_l$ is less than nk. Comparing coefficients, this implies $a_n^k = 0$, so a_n is nilpotent, concluding the induction. □

Problem 4 (D&F 7.4.15)**.** *Let $x^2 + x + 1$ be an element of the polynomial ring $E = \mathbb{F}_2[x]$ and use the bar notation to denote passage to the quotient ring $\mathbb{F}_2[x]/(x^2 + x + 1)$.*

1. *Prove that $\overline{E}$ has 4 elements: $\bar{0}, \bar{1}, \bar{x}$, and $\overline{x+1}$.*
2. *Write out the 4×4 addition table for $\overline{E}$ and deduce that the additive group $\overline{E}$ is isomorphic to the Klein 4-group.*
3. *Write out the 4×4 multiplication table for $\overline{E}$ and prove that $\overline{E}^\times$ is isomorphic to Z_3. Deduce that $\overline{E}$ is a field.*

Solution. Two polynomials in $\mathbb{F}_2[x]$ are the same in $\mathbb{F}_2[x]/(x^2 + x + 1)$ if they differ by a multiple of $x^2 + x + 1$ with multiplier in $\mathbb{F}_2[x]$. The elements 0, 1, x, and $x + 1$ are all elements of $\mathbb{F}_2[x]$ with degree ≤ 1; these represent distinct equivalence classes in quotient, since polynomials of degree lower than 2 are not multiples of any polynomial of higher degree, and they're distinct in $\mathbb{F}_2[x]$. Additionally, these are the only equivalence classes: by induction on n, any polynomial of the form $a_nx^n + \cdots + a_1x + a_0$ where $a_i \in \mathbb{F}_2$ can be written as a multiple of these elements. For degree zero, every polynomial is either 0 or 1, which are parts of $\bar{0}$ and $\bar{1}$. Suppose every polynomial of degree $n - 1$ is in one of the equivalence classes. Then every polynomial of degree n is of the form $p(x) = x^n + p_{n-1}(x)$ for some polynomial p_{n-1} of degree $n - 1$. Accordingly, $p(x) = x(x^{n-1} + p'_{n-1}(x)) + a_0$, where p'_{n-1} is the p_{n-1} without its constant coefficient with all exponents reduced by 1. The polynomial in the parenthesis is of degree $n - 1$, and so is in one of the equivalence classes. x times any element of an equivalence class is again in an equivalence class, so if $a_0 = 0$ we're done. If $a_0 = 1$, p is in the equivalence class according to the rules $\bar{0} + \bar{1} = 1$, $\bar{1} + \bar{1} = \bar{0}$, $\bar{x} + \bar{1} = \overline{x+1}$, and $\overline{x+1} + \bar{1} = \bar{x}$. □

Problem 5 (D&F 7.4.27)**.** *Let R be a commutative ring with $1 \neq 0$. Prove that if a is a nilpotent element of R then $1 - ab$ is a unit for all $b \in R$.*

Solution. By the last problem on the previous homework, ab is nilpotent for all $b \in R$. Similarly, $-x = (-1)x$ is nilpotent if x is. Then $1 - ab$ is of the form $1 + x$, where x is nilpotent; it is therefore a unit. $\square$

Problem 6 (D&F 7.4.30). *Let I be an ideal of the commutative ring R and define*

$$\mathcal{R}(I) = \{r \in R \mid r^n \in I \textit{ for some } n \in \mathbb{Z}^+\}$$

called the radical of I. Prove that $\mathcal{R}(I)$ is an ideal containing I and that $\mathcal{R}(I)/I$ is the nilradical of the quotient ring R/I, i.e. $\mathcal{R}/I = \eta(R/I)$.

Solution. The proof that the nilradical is an ideal translates: if $r^n \in I$ and $s^n \in I$, then $(r-s)^{nm} \in I$ using the binomial theorem and the fact that I is an ideal and therefore closed under internal addition and arbitrary multiplication. $\mathcal{R}(I)$ contains I as those elements of R in the ideal satisfy the membership property with $n = 1$.

The set $\mathcal{R}/I$ is the set cosets of the form rI where $r^n \in I$ for some $n \in \mathbb{Z}^+$. The set $\eta(R/I)$ is the set of cosets of the form rI where r is arbitrary that satisfy the condition

$$(rI)^n = 0 \Leftrightarrow r^n I = 0 \Leftrightarrow r^n \in I \text{ for some } n \in \mathbb{Z}^+$$

The two sets are therefore equal. $\square$

Problem 7 (D&F 7.4.37). *Prove that a subset X of $[0,1]$ is a Zariski closed set iff it is closed in the usual sense as a subset of $\mathbb{R}$.*

Solution. Suppose a subset S of $[0,1]$ is Zariski closed, meaning it is of the form $V(J) = \{x \in [0,1] \mid f(x) = 0 \text{ for all } f \in J\}$, where J is some ideal of the ring R of all continuous functions from $[0,1]$ to $\mathbb{R}$. Since points are closed in $\mathbb{R}$, $f^{-1}(0)$ is a closed subset of $[0,1]$ for any continuous function f, since a continuous preimage of a closed set is closed. $V(J)$ is the intersection of continuous preimages of 0 inside $[0,1]$, and closed sets remain closed under arbitrary intersection, so Zariski closed $\Rightarrow$ closed.

Conversely, suppose X is a closed subset of $[0,1]$. The set $I(X)$ of functions $[0,1] \to \mathbb{R}$ that vanish on X is an ideal by the result of exercise 34. According to exercise 36, $X = V(I(X))$, i.e. X is the Zariski closed set generated by the ideal $I(X)$; in particular, X is Zariski closed. $\square$