Algebra: Chapter 0 Exercises

Chapter 3, Section 3

David Melendez

August 7, 2018

Problem 3.1. Prove that the image of a ring homomorphism $\varphi : R \to S$ is a subring of S. What can you say about φ if its image is an ideal of S? What can you say about φ if its kernel is a subring of R?

Solution. First we'll prove that im φ is a subring of S.

Proof. Suppose $s_1 = \varphi(r_1)$ and $s_2 = \varphi(r_2)$ are elements of im φ. We then have $s_1 + s_2 = \varphi(r_1 + r_2)$ and $s_1 s_2 = \varphi(r_1 r_2)$ since φ is a homomorphism, so both of these are elements of im φ. Additionally, $\varphi(1_R) = 1_S$, making im φ a subring of S. □

If im φ is an ideal of S, then φ is surjective, since the only ideal of S containing the identity 1_S is S itself. If $\ker \varphi$ is a subring of R, then it must contain 1_R, which, combined with the fact that $\ker \varphi$ is an ideal, tells us that $\ker \varphi = R$. Thus φ must be the "zero" morphism $r \mapsto 0$, which isn't actually a ring homomorphism since it does not preserve the identity. ■

Problem 3.2. Let $\varphi : R \to S$ be a ring homomorphism, and let J be an ideal of S. Prove that $I = \varphi^{-1}(J)$ is an ideal of R.

Solution. Suppose $x \in I$ and $r \in R$. We then have $\varphi(rx) = \varphi(r)\varphi(x)$, which is in J since J is an ideal and $\varphi(x) \in J$. The same argument applies to xr (as J is a two-sided ideal), so I is an ideal of R. ■

Problem 3.3. Let $\varphi : R \to S$ be a ring homomorphism, and let J be an ideal of R.

1. Show that $\varphi(J)$ need not be an ideal of S.

   Proof. Let $R = \mathbb{C}$ and $S = \mathbb{H}$ (the quaternions), and let $\iota : \mathbb{C} \to \mathbb{H}$ be the inclusion $a + bi \mapsto a + bi$. The whole of $\mathbb{C}$ is of course an ideal of $\mathbb{C}$, but the "copy" of $\mathbb{C}$ in the quaternions $\iota(\mathbb{C})$ is not an ideal of $\mathbb{H}$, since $(a + bi)j = aj + bk \notin \iota(\mathbb{C})$. □

2. Assume that φ is surjective; then prove that $\varphi(J)$ *is* an ideal of S.

Proof. We already know that $\varphi(J)$ is a subgroup of S since J is a subgroup of R, so let $s \in S$ and $i \in \varphi(J)$. There then exists a $j \in J$ such that $i = \varphi(j)$, and since φ is surjective, there exists an $r \in R$ such that $s = \varphi(r)$. Note, then, that

$$\begin{aligned} si &= \varphi(r)\varphi(j) \\ &= \varphi(rj) \\ &\in \varphi(J), \end{aligned}$$

since rj is in J due to the fact that J is an ideal; hence $\varphi(J)$ is a left-ideal in S. A similar argument shows that $\varphi(J)$ is also a right-ideal in S. □

3. Assume that φ is surjective, and let $I = \ker\varphi$; thus we may identify S with R/I. Let $\overline{J} = \varphi(J)$, an ideal of R/I by the previous point. Prove that

$$\frac{R/I}{\overline{J}} \cong \frac{R}{I+J}.$$

Proof. Denote by ψ the surjective ring homomorphism $R \to \frac{S}{\overline{J}}$ defined by the following chain of homomorphisms:

$$\begin{tikzcd} R \arrow[r, two heads] & \dfrac{R}{I} \arrow[r, two heads] & \dfrac{R/I}{\widetilde{\varphi}^{-1}(\overline{J})} \arrow[r, "\bar\imath"] & \dfrac{S}{\overline{J}} \end{tikzcd}$$

where $\widetilde{\varphi}$ is the isomorphism $r + I \mapsto \varphi(r)$, and $\bar\imath$ is the isomorphism $(r + I) + \widetilde{\varphi}^{-1}(\overline{J}) \mapsto \widetilde{\varphi}(r + I) + \widetilde{\varphi}(\widetilde{\varphi}^{-1}(\overline{J})) = \varphi(r) + \overline{J}$. Hence ψ is defined by $\psi(r) = \varphi(r) + J$. Note, then, that $r \in \ker\psi$ if and only if $\varphi(r) \in \varphi(J)$, if and only if there exists a $j \in R$ such that $\varphi(r) = \varphi(j)$, or equivalently $\varphi(r - j) = 0$, which is true if and only if there exists some $\nu \in \ker\varphi = I$ such that $r - j = \nu$ (equivalently $r = \nu + j$), if and only if $r \in I + J$.

Thus, by the first isomorphism theorem for rings, we have:

$$\frac{R}{I+J} \cong \frac{S}{\overline{J}} \cong \frac{R/I}{\widetilde{\varphi}^{-1}(\overline{J})}.$$

If we identify $\widetilde{\varphi}^{-1}(\overline{J})$ with $\overline{J}$ in the last quotient ring (such an identification can be done in good conscience since doing so using any isomorphism between R/I and S yields isomorphic quotient rings), we can then say that

$$\frac{R}{I+J} \cong \frac{R/I}{\overline{J}}.$$

□

Problem 3.4. Let R be a ring such that every subgroup of $(R, +)$ is in fact an ideal of R. Prove that $R \cong \mathbb{Z}/n\mathbb{Z}$, where n is the characteristic of R.

Solution. Since every subgroup of R is an ideal of R, note that in particular, the subgroup $I = \langle 1_R \rangle$ generated by the identity element is an ideal of R. Note, then, that for all $r \in R$, we have $r 1_R = r \in I$, since $1_R \in I$, and so R is actually cyclic, with order equal to the order of 1_R; in other words, the characteristic n of R. The unique map $\varepsilon : \mathbb{Z} \to R$ is then surjective (since R is generated by 1_R as a group) and has kernel $n\mathbb{Z}$; hence, by the first isomorphism theorem for rings, we have $R \cong \mathbb{Z}/n\mathbb{Z}$. ■

Problem 3.5. Let J be a two-sided ideal of the ring $\mathcal{M}_n(R)$ of $n \times n$ matrices over a ring R. Prove that a matrix $A \in \mathcal{M}_n(R)$ belongs to J if and only if the matrices obtained by placing any entry of A in any position, and 0 elsewhere, belong to J.

Solution. First suppose that $A \in J$. For natural numbers i, j, a, b less than n, We will "find" the matrix B in J with A_{ij} at position a, b.

Let $\eta(p, q)$ the matrix with 1 in the entry at position (q, p) and 0 elsewhere, and let $B = \eta(a, i)A\eta(j, b)$. Let δ be the kronecker delte, and note, then, that

$$\begin{aligned} B_{xy} &= \sum_{k=1}^{n} \eta(a, i)_{xk}(A\eta(j, b))_{ky} \\ &= \delta_{xa}(A\eta(j, b))_{iy} \\ &= \delta_{xa} \sum_{k=1}^{n} A_{ik}\eta(j, b)_{ky} \\ &= \delta_{xa}\delta_{yb}A_{ij}; \end{aligned}$$

hence B is the matrix with A_{ij} at position (a, b) and 0 elsewhere. Since B was obtained by multiplying A on the left and the right by other matrices, it is an element of J, as J is a two-sided ideal. This completes the proof in one direction.

For the proof in the other direction, suppose the matrices obtained by placing any entry of A in ny position, and 0 elsewhere, belong to J. Then, of course, A is the sum of the matrices that have A_{ij} at position (i, j) where i, j range from 1 to $n - 1$; since J is a subgroup of R, this matrix is in J. ■

Problem 3.6. Let J be a two-sided ideal of the ring $\mathcal{M}_n(R)$ of $n \times n$ matrices over a ring R, and let $I \subseteq R$ be the set of $(1, 1)$ entries in J. Prove that I is a two-sided ideal of R and J consists precisely of those matrices whose entries all belong to I.

Solution. First we will prove that I is a two-sided ideal of R. Suppose $r \in I$, and $a \in R$. By exercise 3.5, then, the matrix $r \cdot \eta(1, 1)$ is in J, and so $(r \cdot \eta(1, 1))(a \cdot \eta(1, 1)) = (ra \cdot \eta(1, 1)) \in J$ since J is a right-ideal of $\mathcal{M}_n(R)$, and so $ra \in I$ by the definition of I. Therefore I is a right ideal of R. The same argument can be used to conclude that I is also a left-ideal of R, since J is a left-ideal of $\mathcal{M}_n(R)$.

For the second part of the exercise, suppose first that $A \in J$. Then, by exercise 3.5, we know that for any integers i, j between 1 and $n-1$, there is a matrix in J with A_{ij} at entry $(1,1)$. Thus, $A_{ij} \in I$.

Conversely, suppose A is a matrix whose entries all belong to I. Then, for each entry A_{ij} of A, the matrix $A_{ij} \cdot \eta(i,j)$ is in J by the definition of I and exercise 3.5, so their sum A must also be in J as J is closed under addition (due to it being an ideal). Therefore J consists precisely of those matrices whose entries all belong to I. ■

Problem 3.7. Let R be a ring, and let $a \in R$. Prove that Ra is a left-ideal of R and aR is a right-ideal of R. Prove that a is a left-, resp. right-, unit if and only if $R = aR$, resp $R = Ra$.

Solution. First we will prove that Ra is a left-ideal of R. Suppose $x \in Ra$ so that $x = ra$ for some $r \in R$. Then if $s \in R$, we have $sx = sra = (sr)a \in Ra$. Hence Ra is a left ideal of R. A similar argument shows that aR is a right-ideal of R.

For the second question, note that $R = aR$ (resp. $R = Ra$) if and only if left- resp. right-multiplication by a is surjective, if and only if a is a left- resp. right- ideal of R. ■

Problem 3.8. Prove that a ring R is a division ring if and only if the only left-ideals and right-ideals are $\{0\}$ and R.

In particular, a commutative ring R is a field if and only if the only ideals of R are $\{0\}$ and R.

Solution. Suppose R is a division ring, and I is a right-ideal of R. Of course $\{0\}$ is a right-ideal of R, so suppose $r \neq 0$ is an element of I. Then since R is a division ring, r has a two-sided inverse r^{-1}. Note, then, that since I is an ideal of R, we have $rr^{-1} = 1_R \in I$, and so $I = R$. The same argument applies if I is a left-ideal of R, completing the proof in one direction.

Conversely, suppose the only left- and right-ideals of R are $\{0\}$ and R itself. Then it follows from exercise 3.7 that for all nonzero $a \in R$, we have $aR = R$ and $Ra = R$ (since aR and Ra are nonzero ideals of R), and so a is a left- and right-unit in r; hence every element of R is a two-sided unit, and R is a divison ring. ■

Problem 3.9. Counterpoint to Exercise 3.8: It is *not* true that a ring R is a division ring if and only if its only two-sided ideals are $\{0\}$ and R. A nonzero ring with this property is said to be *simple*; by Exercise 3.8, fields are the only simple *commutative* rings.

Prove that $\mathcal{M}_n(\mathbb{R})$ is simple. (Use Exercise 3.6).

Solution. Suppose J is a nonzero two-sided ideal of $\mathcal{M}_n(\mathbb{R})$. Let α be a nonzero entry of a matrix in J. Then, by exercise 3.5, the matrix with α at the position $(1,1)$ and 0 elsewhere is in J. If we then multiply this matrix with the matrix that has α^{-1} at position $(1,1)$, we then find (using the fact that J is an ideal) that the matrix with 1 at $(1,1)$ and zero elsewhere is in J. Applying 3.5 again and the fact that J is closed under addition, we find that the identity matrix is in J, and so J is the whole of $\mathcal{M}_n(\mathbb{R})$. Therefore $\mathcal{M}_n(\mathbb{R})$ is simple. ■

Problem 3.10. Let $\varphi : k \to R$ be a ring homomorphism, where k is a field and R is a nonzero ring. Prove that φ is injective.

Solution. Suppose $\nu \in k$ is nonzero and $\varphi(\nu) = 0$. Then we have

$$\begin{aligned} 0 &= \varphi(\nu) \\ &= \varphi(\nu)\varphi(\nu^{-1}) \\ &= \varphi(\nu\nu^{-1}) \\ &= \varphi(1) \\ &= 1, \end{aligned}$$

which is a contradiction since R is nonzero. Hence $\nu = 0$ and φ is injective. ■

Problem 3.11. Let R be a ring containing $\mathbb{C}$ as a subring. Prove that there are no ring homomorphisms $R \to \mathbb{R}$.

Solution. Since $\mathbb{C}$ is a subring of R, the element i is then in R. Note, then, that $i^4 = 1$, and so if φ is to be a homomorphism $R \to \mathbb{R}$, we must then have $\varphi(i^4) = 1$. Since this implies $\varphi(i)^4 = 1$, we then know that $\varphi(i)$ is either 1 or -1, since the only fourth roots of 1 in $\mathbb{R}$ are 1 and -1. Either way, we then have, since φ is a homomorphism, that $\varphi(i^2) = \varphi(i)^2 = 1$. But we also have $\varphi(i^2) = \varphi(-1) = -\varphi(1) = -1$, which implies that $1 = -1$. Since this is not true in R, we then know that φ is not a homomorphism, and so there are no ring homomorphisms from R to $\mathbb{R}$. ■

Problem 3.12. Let R be a commutative ring. Prove that the set of nilpotent elements of R is an ideal of R. (This ideal is called the *nilradical* of R.)

Find a noncommutative ring in which the set of nilpotent elements is *not* an ideal.

Solution. First we will prove that the set of nilpotent elements of the commutative ring R is an ideal of R.

Proof. Most of the work here has essentially been done here in 1.6, where we establish that if a, b are nilpotent and commute with each other, then $a + b$ is also nilpotent; hence the set N of nilpotent elements in R form a subgroup of $(R, +)$.

To show that N is an ideal of R, let $\nu \in N$ (so that $\nu^n = 0$) and $r \in R$. Note, then, that $(r\nu)^n = r^n\nu^n = 0$, since R is commutative, and so N is an ideal of R.

□

We already showed in Exercise 1.6, again, that $\mathfrak{gl}_2(\mathbb{R})$ is a noncommutative ring in which the set of nilpotent isn't even a subgroup; the matrices A and B:

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \ ; \ B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \ ;$$

are nilpotent, but their sum is not. ■

Problem 3.13. Let R be a commutative ring, and let N be its nilradical. Prove that R/N contains no nonzero nilpotent elements. (Such a ring is said to be *reduced*).

Solution. Let $\nu + N \in R/N$ be nilpotent. Then, by definition, there exists some integer m such that $0 = (\nu + N)^m = \nu^m + N$. This, of course, means that $\nu^m \in N$, meaning ν^m is nilpotent in R, and so there exists some integer n such that $0 = (\nu^m)^n = \nu^{mn}$. This means that ν is nilpotent and hence in N and so $\nu + N$ is zero in R/N. Therefore, all nilpotent elements in R/N are zero. ■

Problem 3.14. Prove that the characteristic of an integral domain is either 0 or a prime integer. Do you know any ring of characteristic 1?

Solution. We will proceed by proving the contrapositive.

Proof. Let R be a ring of nonzero characteristic n, and suppose n is *not* prime. Let $\varepsilon : \mathbb{Z} \to R$, $m \mapsto m \cdot 1_R$ be the unique ring homomorphism from $\mathbb{Z}$. Since n is not prime, we can decompose it as a product ab of two nonzero integers. Note, then, that $0 = \varepsilon(ab) = \varepsilon(a)\varepsilon(b)$, but $\varepsilon(a)$ and $\varepsilon(b)$ are not zero since a and b are less than the characteristic n of R. Hence R is not an integral domain.

Therefore, if R is an integral domain, its characteristic n is either prime or zero. □

The only ring of characteristic 1 is the ring for which $\ker \varepsilon = 1\mathbb{Z} = \mathbb{Z}$, which is only true for the zero ring. ■

Problem 3.15. A ring R is *Boolean* if $a^2 = a$ for all $a \in R$. Prove that $\mathscr{P}(S)$ is Boolean, for every set S. Prove that every nonzero Boolean ring is commutative and has characteristic 2. Prove that if an integral domain R is Boolean, then $R \cong \mathbb{Z}/2\mathbb{Z}$.

Solution. The proof that $\mathscr{P}(S)$ is boolean is easy: Remember that multiplication in $\mathscr{P}(S)$ is just set intersection; of course, then, $A \cap A = A$ for all $A \subseteq S$, and so $\mathscr{P}(S)$ is Boolean.

If R is a Boolean ring, note that in particular if $r \in R$,

$$\begin{aligned} r + 1 &= (r+1)^2 \\ &= r^2 + r + r + 1 \\ &= r + r + r + 1, \end{aligned}$$

which implies that

$$r = -r$$

. This, of course, implies that $1 + 1 = 1 + (-1) = 0$, and so the characteristic of R is 2.

Additionally, we have, for all $a, b \in R$,

$$\begin{aligned} 0 &= a + b - (a+b) \\ &= (a+b)^2 - (a+b) \\ &= a^2 + ab + ba + b^2 - (a+b) \\ &= a + ab + ba + b - (a+b) \\ &= ab + ba \\ &= ab - ba, \end{aligned}$$

and so $ab = ba$ for all $a, b \in R$, showing that R is commutative. ■

Problem 3.16. Let S be a set and $T \subseteq S$ a subset. Prove that the subsets of S contained in T form an ideal of the power set ring $\mathscr{P}(S)$. Prove that if S is finite, then *every* ideal of $\mathscr{P}(S)$ is of this form. For S infinite, find an ideal of $\mathscr{P}(S)$ that is *not* of this form.

Solution.

1. The subsets of S contained in T form an ideal of the power set ring

   Proof. First, let T be a subset of S, and let $A, B \in \mathscr{P}(T)$. Then of course $A + B = (A \cup B) \setminus (A \cap B)$ is a subset of T. Additionally, the null set is the identity with respect to this addition, and it is also in $\mathscr{P}(T)$. Hence $(\mathscr{P}(T), +)$ is a subgroup of $(\mathscr{P}(S), +)$.
   Now, to show that $\mathscr{P}(T)$ is an ideal of $\mathscr{P}(S)$, let A be a subset of T and let α be a subset of S. Then $\alpha \cap A \subseteq A \subseteq T$, and so $\alpha \cap A \in \mathscr{P}(S)$. Since $\mathscr{P}(S)$ is commutative, this shows that $\mathscr{P}(T)$ is an ideal.

   □

2. If S is finite, then *every* ideal of $\mathscr{P}(S)$ is of this form.

   Proof. Suppose $\mathcal{J} \subseteq \mathscr{P}(S)$ is an ideal of $\mathscr{P}(S)$. Let $J \in \mathscr{P}(S)$ be the union of all sets in $\mathcal{J}$. Clearly $A \in \mathcal{J}$ implies $A \subseteq J$, so suppose conversely that $A \subseteq J$. Let $\mathcal{I} \subseteq \mathcal{J}$ be the set of all sets in $\mathcal{J}$ that meet A (i.e. have a non-empty intersection with A). Since $A \subseteq J$, we know that there are sets in $\mathcal{J}$ whose union contains A, and so

   $$\begin{aligned} A &\subseteq \bigcup \mathcal{I} \\ &\in \mathcal{J}. \end{aligned}$$

   Here, the first line is clear, and the second line is true for two reasons: Firstly, the union of two sets can be expressed in terms of symmetric differences and unions of those two sets ($X \cup Y = (X + Y) + (X \cap Y)$), and so any finite union can be expressed in these terms, although this is difficult to write explicitly. Secondly, ideals are closed under addition (here the symmetric difference) and multiplication (here intersection), so the union of all sets in $\mathcal{I}$, for the reason stated above, is of course in $\mathcal{J}$. We then have, finally:

   $$\begin{aligned} A &= A \cap \bigcap \mathcal{I} \\ &\in \mathcal{J}, \end{aligned}$$

   where the first line is true because $A \subseteq \bigcup \mathcal{I}$, and the second line is true because $\mathcal{J}$ is an ideal, $\bigcup \mathcal{I} \in \mathcal{J}$, and $A \in \mathscr{P}(S)$. Thus $A \subseteq J$ implies $A \in \mathcal{J}$.
   We've just proven that $A \in \mathcal{J}$ if and only if $A \subseteq J$; it then follows that $\mathcal{J} = \mathscr{P}(J)$, as desired. □

3. For S infinite, find an deal of $\mathscr{P}(S)$ that is *not* of this form.
   I'm not immediately sure how to construct an explicit counterexample, but the proof

above fails in the case that S is infinite, since $\mathcal{J}$ being infinite would make $\mathcal{I}$ potentially infinite, and so it's not at all clear that you can write the union of infinitely many sete in terms of intersections and symmetric differences. In fact, even if such a feat were possible, the proof would still fail, since the algebraic structures we're dealing with are only required to be closed under *finite* applications of the relevant operations.

■