

**Homework 4\*\*\*** [With some annotations by BHP]

1. Let's call the algebra on the set of natural numbers  $\mathbf{N}$  with the addition and multiplication operations  $\mathbf{A}$ , and the homomorphism from  $\mathbf{A}$  to  $\mathbf{Parity}$ ,  $F : \mathbf{A} \rightarrow \mathbf{Parity}$ .

(a) According to this function, members the carrier set of  $\mathbf{A}$  (namely  $\mathbf{N}$ ) are mapped onto either even or odd, the two members of the carrier set of the algebra  $\mathbf{Parity}$  (since all natural numbers are either even or odd). Members of the operations **plus** and **times** in  $\mathbf{A}$  are mapped onto the corresponding operations **plus** and **times** in  $\mathbf{Parity}$ .

Let  $n$  and  $m$  stand for any natural number (and they need not be distinct from each other); then even numbers and odd numbers can be represented as follows: Even numbers:  $2n, 2m$ , etc.; odd number:  $2n+1, 2m+1$ , etc.

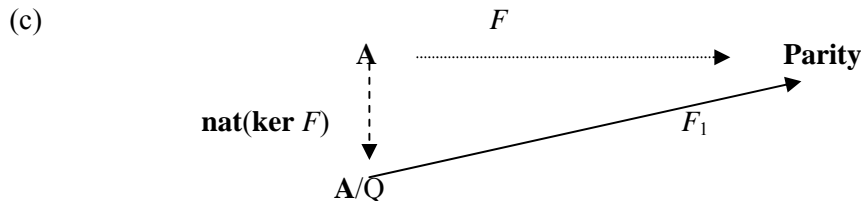
$$\begin{aligned} \mathbf{plus}(2n,2m) &= 2(n+m); & \mathbf{plus}(2n+1,2m+1) &= 2(n+m+1); & \mathbf{plus}(2n,2m+1) &= 2(n+m)+1 \\ \mathbf{times}(2n,2m) &= 4(nm); & \mathbf{times}(2n+1,2m+1) &= 2(2nm+n+m)+1; & \mathbf{times}(2n,2m+1) &= 2(nm+n) \end{aligned}$$

$$\begin{aligned} Q = \ker F = \{ & \langle 2n, 2m \rangle, \langle 2n+1, 2m+1 \rangle, \langle \mathbf{plus}(2n, 2m), \mathbf{plus}(2n, 2m) \rangle, \langle \mathbf{plus}(2n, 2m), \mathbf{plus}(2n+1, 2m+1) \rangle, \\ & \langle \mathbf{plus}(2n, 2m), \mathbf{times}(2n, 2m) \rangle, \langle \mathbf{plus}(2n, 2m), \mathbf{times}(2n, 2m+1) \rangle, \\ & \langle \mathbf{plus}(2n+1, 2m+1), \mathbf{plus}(2n+1, 2m+1) \rangle, \langle \mathbf{plus}(2n+1, 2m+1), \mathbf{times}(2n, 2m) \rangle, \\ & \langle \mathbf{plus}(2n+1, 2m+1), \mathbf{times}(2n, 2m+1) \rangle, \langle \mathbf{times}(2n, 2m), \mathbf{times}(2n, 2m) \rangle, \\ & \langle \mathbf{times}(2n, 2m), \mathbf{times}(2n, 2m+1) \rangle, \langle \mathbf{times}(2n, 2m+1), \mathbf{times}(2n, 2m+1) \rangle, \\ & \langle \mathbf{plus}(2n, 2m+1), \mathbf{plus}(2n, 2m+1) \rangle, \langle \mathbf{plus}(2n, 2m+1), \mathbf{times}(2n+1, 2m+1) \rangle, \\ & \langle \mathbf{times}(2n+1, 2m+1), \mathbf{times}(2n+1, 2m+1) \rangle \} \end{aligned}$$

\*\*\* **Note from BHP:** I think what's there is all correct, but it isn't the way I would have written down what the kernel consists of. I would say  $Q = \ker F = \{ \langle x, y \rangle \mid x, y \in \mathbb{N}, \text{ and } x, y \text{ are both odd or both even} \}$ , or equivalently,  $\{ \langle x, y \rangle \mid x, y \in \mathbb{N}, \text{ and } x, y \text{ have the same parity} \}$ . \*\*\*

(b) The corresponding quotient algebra  $\mathbf{A}/Q$   
 $= \{ \{ \{ 2n \}, \{ 2n+1 \} \}, \{ \mathbf{plus}(2n, 2m), \mathbf{plus}(2n+1, 2m+1), \mathbf{times}(2n, 2m), \mathbf{times}(2n, 2m+1) \}, \{ \mathbf{plus}(2n, 2m+1), \mathbf{times}(2n+1, 2m+1) \} \}$

\*\*\* **Note from BHP:** This is not quite right. The carrier has just two elements, which are the two equivalence classes. So I would write the carrier as  $\{ [[ 0 ]], [[ 1 ]]$ . And then to complete the algebra, we need to draw the two operation tables (they are just  $2 \times 2$  tables). \*\*\*



2. Algebra of the symmetries of the square

\*\*\* **Note from BHP:** In the reasoning below, which is all correct and well-put, there is one peculiar bit of terminology – all of the operations

R', H, V, D, D' are referred to as "180° rotations", when in fact only R' should be referred to that way. What is meant is "operations (other than I) which are their own inverses". \*\*\*

(a)

◦	I	R	R'	R''	H	V	D	D'
I	I	R	R'	R''	H	V	D	D'
R	R	R'	R''	I	D	D'	V	H
R'	R'	R''	I	R	V	H	D'	D
R''	R''	I	R	R'	D'	D	H	V
H	H	D'	V	D	I	R'	R''	R
V	V	D	H	D'	R'	I	R	R''
D	D	H	D'	V	R	R''	I	R'
D'	D'	V	D	H	R''	R	R'	I

(b) The three different subgroups with exactly four elements and their operation tables.

Subgroups have to meet the following criteria of a group:

G1:  $G$  is an algebra (i.e. completely defined and  $G$  closed under the single binary operation.

G2: The single binary operation has to be associative, i.e. it is immaterial in what order repeated applications are made.

G3:  $G$  contains an identity element.

G4: Each element in  $G$  has an inverse element.

In addition, they also have to meet the following criteria of a subalgebra:

SubG1: The carrier of the subalgebra is a subset of the carrier of the algebra.

SubG2: For every operator in the algebra, the carrier set of the subalgebra is closed w.r.t. the operation .

SubG3: For every operator in the algebra, the operation restricted to the carrier set of the subalgebra equals the operation in the subalgebra.

The symmetries of the square meet the criteria of a group (and of an algebra):

G1: It's completely defined and its carrier set is closed under the operation ◦.

G2: As shown in the full operation table, the operation ◦ "and then do..." is not commutative. It is however associative.

G3: I is the identity element in the carrier set.

G4: Each element in the carrier set has an inverse element (since a square is a completely symmetric structure).

Its subgroup is then a group with

(i) a subset of  $\{I, R, R', R'', H, V, D, D'\}$  is its carrier set,

(ii) this subset is closed w.r.t. the operation ◦ (there's only one, this being a group).

(iii) The operator ◦ restricted to the carrier set of this subset equals the operation in the subalgebra.

Given (ii) and (iii), the subgroups we're looking for are therefore subgroups with a carrier set that contains pairs of 180° rotations: I-R', R'-R'', H-V, D-D'. The carrier sets all have to contain the identity element I (by G3), hence its 180° counterpart R'. This gives us three different subgroups with a carrier set of four elements:  $\langle\{I, R, R', R''\}, \circ\rangle$ ,  $\langle\{I, R', H, V\}, \circ\rangle$ ,  $\langle\{I, R', D, D'\}, \circ\rangle$ . Their operation tables are given below:

◦	I	R	R'	R''
I	I	R	R'	R''
R	R	R'	R''	I
R'	R'	R''	I	R
R''	R''	I	R	R'

◦	I	R'	H	V
I	I	R'	H	V
R'	R'	I	V	H
H	H	V	I	R'
V	V	H	R'	I

◦	I	R'	D	D'
I	I	R'	D	D'
R'	R'	I	D'	D
D	D	D'	I	R'
D'	D'	D	R'	I

(c) The five different subgroups with exactly two elements and their operation tables.

Subgroups are those with a carrier set consisting of the identity element I and any of the 180° operations:  $\langle \{I, R'\}, \circ \rangle$ ,  $\langle \{I, H\}, \circ \rangle$ ,  $\langle \{I, V\}, \circ \rangle$ ,  $\langle \{I, D\}, \circ \rangle$ ,  $\langle \{I, D'\}, \circ \rangle$ .

◦	I	R'
I	I	R'
R'	R'	I

◦	I	H
I	I	H
H	H	I

◦	I	D
I	I	D
D	D	I

◦	I	V
I	I	V
V	V	I

◦	I	D'
I	I	D'
D'	D'	I

(d) Of the subgroups in (b),  $\langle \{I, R', H, V\}, \circ \rangle$ ,  $\langle \{I, R', D, D'\}, \circ \rangle$  are isomorphic. In fact, as long as the identity element stays put (is identical in both subgroups), all the possible 1-to-1 onto mappings are isomorphisms, since the movements R', H, V, D, D' are all 180° movements. (I believe there's a typo in the answer key to this problem: it says in one place R instead of R').

(e) For the subgroup  $\langle \{I, R, R', R''\}, \circ \rangle$ , its only non-trivial automorphism is a function that maps the two non-180° movements R and R'' to each other. Mapping R' to anything other than itself will not do, since the identity element I has to be mapped onto itself, and the other two movements are not 180° equivalents of R'. This contrasts with the case of the other subgroups  $\langle \{I, R', H, V\}, \circ \rangle$ ,  $\langle \{I, R', D, D'\}, \circ \rangle$ , where every movement H, V, D, D' is a 180° movement. In this case, mapping any of these movements onto any of the other movements (in the same subgroup) will yield an isomorphism (and automorphism).

⊗ I understand that for each of these subgroups there are three movements (R', H, V for the first subgroup, and R', D, D' for the second) which can be mapped onto any of the other two movements (since mapping onto itself is a trivial automorphism), but I don't see how there are five possible such combinations, as suggested in the answer key, and not six (the product of three times two).

\*\*\* Note added by BHP: No, book is right. Consider the group with  $\{I, R', H, V\}$  R' can map onto any of the three non-I operations, including itself; once you fix what R' maps onto, then H can map onto either of the remaining two; then V must map onto the remaining one. So there are  $3 \times 2 = 6$  automorphisms in all, of which one is the trivial one and five are non-trivial. Note that you don't have to prevent R' from mapping onto itself altogether, since it's non-trivial as long as they don't *all* map onto themselves. \*\*\*

(f) A homomorphism of one of the subgroups of (b) with one of the subgroups of (c).

Considering the subgroups  $\langle \{I, R, R', R''\}, \circ \rangle$  and  $\langle \{I, R'\}, \circ \rangle$ ,  $f$  is a homomorphism if  $f(I) = I$ ,  $f(R') = I$ ,  $f(R) = R'$ ,  $f(R'') = R'$  (basically, I and its 180° degree counterpart map onto the identity

element, and the other two movements, onto the non-identity element in the (c) subgroup's carrier set).

In fact, given that all subgroups in (c) are isomorphic, the same mapping  $f$  is a homomorphism from  $\langle \{I, R, R', R''\}, \circ \rangle$  to any of these subgroups.

A similar mapping (where  $f(I) = I, f(X) = I, f(Y) = W, f(Z) = W; W, X, Y, Z$  are all movements  $180^\circ$  removed from the identity element) is a homomorphism from the isomorphic  $\langle \{I, R', H, V\}, \circ \rangle$  and  $\langle \{I, R', D, D'\}, \circ \rangle$  to the isomorphic subgroups  $\langle \{I, R'\}, \circ \rangle, \langle \{I, H\}, \circ \rangle, \langle \{I, V\}, \circ \rangle, \langle \{I, D\}, \circ \rangle, \langle \{I, D'\}, \circ \rangle$ . In this case, since all movements involved are  $180^\circ$  of each other and of the identity element, any of the movements  $R', H, V,$  or  $R', D, D'$  can be the other element (besides  $I$ ) to be mapped onto  $I$  in the smaller subgroup, and there should be 5 such homomorphisms from each of the subgroups  $\langle \{I, R', H, V\}, \circ \rangle$  and  $\langle \{I, R', D, D'\}, \circ \rangle$  (if the answer key to (e) is correct).

\*\*\***BHP**: I think there are just *three* such *onto* homomorphisms from e.g.  $\{I, R', H, V\}$  onto e.g.  $\{I, V\}$ . The only freedom of choice is which non- $I$  element in the 4-member one to map onto  $I$  in the 2-member one. \*\*\*

### 3. Handout questions

p. 2: Why  $A^0 = \{\emptyset\}$ ?

$A^n = A \times A \times \dots = \{ \langle a_1, \dots, a_n \rangle \mid a_i \in A \}$  ( $n$  = the number of the sets—or times the same set—are related)

$\langle a, b \rangle = \{ \{a\}, \{a, b\} \}$

When  $n = 0$ , there is no set being related, and the “ordered pairs” (which are themselves sets) in this case, can be made explicit using the same rewriting rule that rewrites ordered pairs as sets. Since there is no set or member being related, the ordered pairs form an empty set, and since the Cartesian product is the set of all ordered pairs,  $A^0$  corresponds to  $\{\emptyset\}$ .

p. 4: The empty set trivially closed under all operations except for 0-ary operations, since there is no member in the empty set to operate on. 0-ary operations, however, return a constant for any member, and therefore, would give a value set comprising the constant, which is not present in the domain empty set. The null set is thus not closed under 0-ary operations.

p. 4: Show that the intersection of two subalgebras of algebra  $\mathbf{A}$  is also a subalgebra of  $\mathbf{A}$ .

Let's consider the two subalgebras  $\mathbf{A}' \langle A', \Omega \rangle$  and  $\mathbf{A}'' \langle A'', \Omega \rangle$ . As subalgebras of  $\mathbf{A} \langle A, \Omega \rangle$ ,

(i)  $A' \subseteq A$  and  $A'' \subseteq A$ .

(ii) for every operator  $\omega \in \Omega(n)$  and for every  $n$ -tuple  $\langle a'_1, \dots, a'_n \rangle \in A'^n$ ,  $\omega_{\mathbf{A}}(a'_1, \dots, a'_n) \in A'^n$ .

Likewise, for every  $n$ -tuple  $\langle a''_1, \dots, a''_n \rangle \in A''^n$ ,  $\omega_{\mathbf{A}}(a''_1, \dots, a''_n) \in A''^n$ .

(iii) for every operator  $\omega \in \Omega$ ,  $\omega_{\mathbf{A}}|_{A'} = \omega_{\mathbf{A}'}$  and  $\omega_{\mathbf{A}}|_{A''} = \omega_{\mathbf{A}''}$ .

The intersection algebra  $\mathbf{B} = \mathbf{A}' \cap \mathbf{A}''$ :

(i) has a carrier set  $A' \cap A'' \subseteq A$ , since  $A' \subseteq A$  and  $A'' \subseteq A$ .

(ii) for every operator  $\omega \in \Omega(n)$  and for every  $n$ -tuple  $\langle b_1, \dots, b_n \rangle \in B^n$ ,  $\omega_{\mathbf{A}}(b_1, \dots, b_n) \in B^n$ , since for every  $n$ -tuple  $\langle a'_1, \dots, a'_n \rangle \in A'^n$ ,  $\langle a''_1, \dots, a''_n \rangle \in A''^n$ ,  $\omega_{\mathbf{A}}(a'_1, \dots, a'_n) \in A'^n$  and  $\omega_{\mathbf{A}}(a''_1, \dots, a''_n) \in A''^n$  and  $B = A' \cap A''$ .

(iii) for every operator  $\omega \in \Omega$ ,  $\omega_{\mathbf{A}}|_B = \omega_{\mathbf{B}}$ , since  $\omega_{\mathbf{A}}|_{A'} = \omega_{\mathbf{A}'} = \omega_{\mathbf{A}}|_{A''} = \omega_{\mathbf{A}''}$  and by idempotent law of intersection.

p. 4: A homomorphism  $F: \mathbf{A} \rightarrow \mathbf{B}$  is called an isomorphism between  $\mathbf{A}$  and  $\mathbf{B}$  if the inverse relation  $f^{-1}: B \rightarrow A$  is a function and it is a homomorphism. Why is it not enough to require only that  $f^{-1}: A \rightarrow B$  be a function?

⊗ I thought at first that this was a trick question, and that there must be something wrong with my initial answer.

It is. If  $f: \mathbf{A} \rightarrow \mathbf{B}$  is a homomorphism, then  $f: A \rightarrow B$ . And if moreover  $f^{-1}: B \rightarrow A$ , the relation between  $A$  and  $B$  is a one-to-one onto mapping. Furthermore,  $f(\omega_A(a)) = \omega_B(f(a)) = \omega_B(b)$ . Since  $f^{-1}: B \rightarrow A$  is a one-to-one onto mapping,  $f^{-1}(\omega_B(b)) = \omega_A(a)$ . It is therefore sufficient for the inversion relation between the carrier sets to be a function for  $F: \mathbf{A} \rightarrow \mathbf{B}$  to be an isomorphism.

p. 5: That  $F: \text{Mod4} \rightarrow \text{Mod2} : f(0) = 0, f(1) = 1, f(2) = 1, f(3) = 0$  is not a homomorphism can easily be shown by the drawing up operation tables for either binary operation:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

+	0	1
0	0	1
1	1	0

$$f(1+1) \text{ in Mod4} = 1; f(1)+f(1) \text{ in Mod2} = 0 \rightarrow f(1+1) \text{ in Mod4} \neq f(1)+f(1) \text{ in Mod2}.$$