1.5 - Quotient Algebras and Homomorphisms

Nicholas McConnell

(Universal Algebra)

The material and exposition for this lesson follows an imaginary textbook on Dozzie Abstract Algebra.

Let Φ be a congruence relation on an Ω-algebra A. Our goal is to show that the set A/Φ of congruence classes is actually an Ω-algebra.

If $a \in A$, the congruence class with a is denoted $\overline{a}_\Phi$, or $\overline{a}$ if Φ is clearly under discussion. Thus $\overline{a} = \overline{b}$ if and only if $a\Phi b$. For each $\omega \in \Omega(0)$, we take $(\omega_{A/\Phi}) = \overline{(\omega_A)}$. Now suppose $n \geq 1$ and $\omega \in \Omega(n)$. Then define ω as follows:

$$(\omega\overline{a}_1\overline{a}_2 \ldots \overline{a}_n) = \overline{(\omega a_1 a_2 \ldots a_n)}$$

for $a_1, a_2, \ldots a_n \in A$. We need to know that ω is well-defined on A/Φ [its result does not depend on the representatives used for the operands in A/Φ]. However, this follows from the fact that Φ is a congruence relation, thus a subalgebra of $A \times A$. So if $\overline{b}_i = \overline{a}_i$ for $i = 1, 2, \ldots n$, then $\overline{(\omega a_1 a_2 \ldots a_n)} = \overline{(\omega b_1 b_2 \ldots b_n)}$.

Section 9 shows that all identities that hold for A also hold for A/Φ. Right now, we think of A as a set equipped with operations without any identities required. It is called the **quotient algebra of A given by Φ**.

NOTE You should take the time to verify that if Ω-algebras are groups, and N is the normal subgroup in G corresponding to the congruence relation Φ, then the quotient group G/N is the same as G/Φ just defined. Same for R-modules and submodules; rings and ideals; and Boolean algebras and filters.

The definition of A/Φ may appear to resemble a homomorphism. Well, it does. If Φ is a congruence relation on A, define $\pi : A \to A/\Phi$ by $\pi(a) = \overline{a}$ for all $a \in A$. Then π is a homomorphism:

$$\pi(\omega a_1 a_2 \ldots a_n) = \overline{(\omega a_1 a_2 \ldots a_n)} = (\omega\overline{a}_1\overline{a}_2 \ldots \overline{a}_n) = (\omega\pi(a_1)\pi(a_2) \ldots \pi(a_n))$$

and is clearly surjective, because every element of A/Φ can be represented by an element of A. π is called the **canonical epimorphism [natural homomorphism] of A into A/Φ**. Notice that $a\Phi b$ in A if and only if $\overline{a} = \overline{b}$ in A/Φ, that is, $\pi(a) = \pi(b)$. This leads to the following definition.

DEFINITION *If $f : A \to B$ is a homomorphism of Ω-algebras, the* ***kernel*** *of f is defined to be the relation* $\{(a_1, a_2) \in A \times A \mid f(a_1) = f(a_2)\}$.

It is clear that f is injective if and only if its kernel is 1_A. The kernel informally measures how far f is from being injective.

Take another look at the canonical epimorphism $\pi : A \to A/\Phi$. What is its kernel? Well, (a, b) is in the kernel of π if and only if $\pi(a) = \pi(b)$, which is true if and only if $a\Phi b$, as we saw before the definition. So the kernel of π is Φ. This means that every congruence relation on A is the kernel of some homomorphism from A. Conversely, a kernel is always a congruence relation:

THEOREM 1.9 *If $f : A \to B$ is a homomorphism of Ω-algebras, then the kernel Θ of f is a congruence relation on A.*

Notice that if $f : G \to H$ is a homomorphism of groups, its kernel [as a relation] corresponds to the normal subgroup $N = \{a \in G \mid f(a) = e\}$, which is also called its kernel.

Proof of Theorem 1.9. Θ is obviously an equivalence relation on A. Now suppose $\omega \in \Omega(n)$ and $a_1, a_2, \dots a_n, b_1, b_2, \dots b_n \in A$ with $a_i \Theta b_i$ for $1 \leq i \leq n$. Then $f(a_i) = f(b_i)$ for all i, and hence,

$$f(\omega a_1 a_2 \dots a_n) = (\omega f(a_1) f(a_2) \dots f(a_n)) = (\omega f(b_1) f(b_2) \dots f(b_n)) = f(\omega b_1 b_2 \dots b_n)$$

therefore, $(\omega a_1 a_2 \dots a_n) \Theta (\omega b_1 b_2 \dots b_n)$, and Θ is a congruence relation. ■

An Ω-algebra B is said to be a **homomorphic image** of an Ω-algebra A if there exists a surjective homomorphism $A \to B$. The canonical epimorphism shows that A/Φ is a homomorphic image of A, for every congruence relation Φ. To see that every homomorphic image actually looks like one of those, we develop the dual of Theorem 1.5, where injectivity and surjectivity are exchanged.

THEOREM 1.10 (INJECTIFICATION) *Let $f : A \to B$ be a homomorphism of Ω-algebras and Φ a congruence relation on A. If $\pi : A \to A/\Phi$ is the canonical epimorphism, then:*

(1) *There exists a homomorphism $\overline{f} : A/\Phi \to B$ such that $f = \overline{f}\pi$ [in other words, that $\overline{f}(\overline{a}) = f(a)$ for all $a \in A$] if and only if $\Phi \subseteq \ker f$.*

If the equivalent conditions in (1) hold, then

(2) *$\overline{f}$ is unique;*

(3) *$\overline{f}$ is injective if and only if $\Phi = \ker f$;*

(4) *$\overline{f}$ is surjective if and only if f is surjective.*

Here's the idea: $\ker f$ tells how much information is lost through f. By changing the domain to A/Φ, some of the information ends up never existing in the first place. (4) shows that surjectivity is not affected, and (3) shows that injectivity comes from dividing the domain by the whole kernel.

Proof of Theorem 1.10. (1) Suppose $\Phi \subseteq \ker f$. Now define $\overline{f} : A/\Phi \to B$ by $\overline{f}(\overline{a}) = f(a)$. This map is well-defined because $\Phi \subseteq \ker f$, and hence, if $\overline{a} = \overline{b}$ in A/Φ, then $f(a) = f(b)$. $\overline{f}$ is a homomorphism because

$$\overline{f}(\omega \overline{a}_1 \overline{a}_2 \dots \overline{a}_n) = \overline{f}(\overline{\omega a_1 a_2 \dots a_n}) = f(\omega a_1 a_2 \dots a_n)$$

$$= (\omega f(a_1) f(a_2) \dots f(a_n)) = (\omega \overline{f}(\overline{a}_1) \overline{f}(\overline{a}_2) \dots \overline{f}(\overline{a}_n))$$

for $\omega \in \Omega(n)$ and $a_1, a_2, \dots a_n \in A$. Also, $f(a) = \overline{f}(\overline{a}) = \overline{f}\pi(a)$, so that $f = \overline{f}\pi$. Conversely, if $\overline{f} : A/\Phi \to B$ is a homomorphism such that $f = \overline{f}\pi$, then whenever $a \Phi b$, $\pi(a) = \pi(b)$, so that $f(a) = \overline{f}\pi(a) = \overline{f}\pi(b) = f(b)$ and $(a, b) \in \ker f$. Thus $\Phi \subseteq \ker f$.

(2) Suppose $\overline{f}' : A/\Phi \to B$ is also a homomorphism satisfying $f = \overline{f}'\pi$. Then $\overline{f}\pi = \overline{f}'\pi$. Since π is surjective, $\overline{f} = \overline{f}'$ follows, and $\overline{f}$ is unique.

(3) Suppose $\overline{f}$ is injective. We already know that $\Phi \subseteq \ker f$, so let $(a, b) \in \ker f$, and we show that $a\Phi b$. Well, $f(a) = f(b)$ by definition. Hence, $\overline{f}\pi(a) = \overline{f}\pi(b)$, so that $\pi(a) = \pi(b)$ since $\overline{f}$ is injective. This implies $a\Phi b$. Hence $\ker f \subseteq \Phi$ and $\Phi = \ker f$. Conversely, if $\Phi = \ker f$ and $\overline{f}(\overline{a}) = \overline{f}(\overline{b})$, then $f(a) = \overline{f}\pi(a) = \overline{f}\pi(b) = f(b)$. Thus $(a, b) \in \ker f$, which is Φ, by hypothesis, hence $a\Phi b$ and $\overline{a} = \overline{b}$. Therefore $\overline{f}$ is injective.

(4) For each $b \in B$, there exists $a \in A$ such that $f(a) = b$ if and only if there exists $a \in A$ such that $\overline{f}(\overline{a}) = b$, that is, if there exists $\overline{a} \in A/\Phi$ such that $\overline{f}(\overline{a}) = b$. So the images of f and $\overline{f}$ are the same subalgebra of B, and of course, one is surjective if and only if the other is. ■

If f is surjective and $\Phi = \ker f$, then the map $\overline{f}$ given by Theorem 1.10 is injective and surjective, so that it is an isomorphism. Hence:

COROLLARY 1.11 (FIRST ISOMORPHISM THEOREM) *If $f : A \to B$ is a surjective homomorphism with kernel Θ, then $A/\Theta \cong B$.*

Thus every homomorphic image of A is actually isomorphic to A/Θ, for some congruence relation Θ.

Note that the identity map $1_A : A \to A$ is surjective with kernel 1_A. [It should not be ambiguous when 1_A refers to the identity map, and when it refers to the identity relation.] By the First Isomorphism Theorem, $A/1_A \cong A$ follows.

What is $A/(A \times A)$, on the other hand? If $A = \emptyset$, this quotient is empty, of course. Now suppose $A \neq \emptyset$. Since $A \times A$ is the relation that holds for all pairs of elements of A, there is a single congruence class in $A/(A \times A)$. It follows that $A/(A \times A) \cong T(\Omega)$.

Subalgebras and Quotient Algebras of Quotient Algebras

What can be said about subalgebras of A/Φ? Let C be a subalgebra of A/Φ and $B = \{a \in A \mid \overline{a} \in C\}$ be the union of the congruence classes in C. It is clear that B is a Φ-invariant subalgebra of A. Now define $f : B \to C$ by $f(a) = \overline{a}$. For each $\overline{a} \in C$, $a \in B$ by definition and $\overline{a} = f(a)$ so f is surjective. Clearly f is a homomorphism.

What's the kernel of f? Well, $f(a_1) = f(a_2)$ if and only if $\overline{a_1} = \overline{a_2}$, which holds if and only if $a_1\Phi a_2$ in A [because C consists of congruence classes of Φ]. So $f(a_1) = f(a_2)$ for $a_1, a_2 \in B$ if and only if $a_1\Phi a_2$ in A. Furthermore, the kernel of f is $\Phi \cap (B \times B)$ [or $\Phi \cap B^2$], the restriction of Φ to B. By Corollary 1.11, $B/(\Phi \cap B^2) \cong C$. In fact, $B/(\Phi \cap B^2)$ *is* C, because B is Φ-invariant, and hence, $B/(\Phi \cap B^2)$ consists of the congruence classes of Φ contained in B.

So, the subalgebras of A/Φ are of the form $B/(\Phi \cap B^2)$ with B a Φ-invariant subalgebra of A. What can we say about $B/(\Phi \cap B^2)$ if B is *any* subalgebra of A? The idea is to "complete" the half-full congruence classes. Recall that

$B\Phi = \{a \in A \mid a\Phi b \text{ for some } b \in B\}$ is the union of the congruence classes of Φ that meet B. Exercise 4(a) of the last section shows that $B\Phi$ is a Φ-invariant subalgebra of A. Hence, $B\Phi/(\Phi \cap (B\Phi)^2)$ is a subalgebra of A/Φ. Since all we did to $B/(\Phi \cap B^2)$ was add to the congruence classes, we expect the Ω-algebra structure to remain unchanged. This is indeed the case:

THEOREM 1.12 (SECOND ISOMORPHISM THEOREM) *Let B be a subalgebra of A and Φ a congruence relation on A. Then $B/(\Phi \cap B^2)$ is isomorphic to the subalgebra $B\Phi/(\Phi \cap (B\Phi)^2)$ of A/Φ.*

Since $B\Phi$ is Φ-invariant, one could abbreviate $B\Phi/(\Phi \cap (B\Phi)^2)$ as $B\Phi/\Phi$.

Proof of Theorem 1.12. Define $f : B \to B\Phi/(\Phi \cap (B\Phi)^2)$ by $f(b) = \bar{b}_\Phi$. Then clearly f is a homomorphism. Every element of $B\Phi/(\Phi \cap (B\Phi)^2)$ is of the form $\bar{c}_\Phi$ with $c \in B\Phi$. By definition, there exists $b \in B$ with $b\Phi c$, and hence $\bar{c}_\Phi = \bar{b}_\Phi = f(b)$. Therefore, f is surjective.

We claim that $\ker f = \Phi \cap B^2$, so that the statement $B/(\Phi \cap B^2) \cong B\Phi/(\Phi \cap (B\Phi)^2)$ will follow from Corollary 1.11. If $f(a) = f(b)$, then $\bar{a}_\Phi = \bar{b}_\Phi$, and hence, $a\Phi b$. However, a and b must be in B for $f(a)$ and $f(b)$ to exist. Therefore, $(a, b) \in \Phi \cap B^2$. Conversely, if $(a, b) \in \Phi \cap B^2$, then $(a, b) \in \Phi$, so that $\bar{a}_\Phi = \bar{b}_\Phi$ and $f(a) = f(b)$. Therefore, $\ker f = \Phi \cap B^2$. ■

Now to ask about quotient algebras of A/Φ. To do this, suppose Φ and Θ are congruence relations on A with $\Phi \subseteq \Theta$. Then define

$$\Theta/\Phi = \{(\bar{a}_\Phi, \bar{b}_\Phi) \in A/\Phi \times A/\Phi \mid a\Theta b\}$$

Since $\Phi \subseteq \Theta$, it turns out that whether an element of $A/\Phi \times A/\Phi$ is in Θ/Φ doesn't depend on the choice of congruence class representatives. It is also clear that Θ/Φ is a congruence relation on A/Φ. Now consider the map from congruence relations on A containing Φ to congruence relations on A/Φ, sending each Θ containing Φ to the relation Θ/Φ just defined. Exercise 6 shows that this is a bijective map.

Hence, every congruence relation on A/Φ is of the form Θ/Φ. What is the structure of the quotient $(A/\Phi)/(\Theta/\Phi)$? Well, we have basically glued Φ's congruence classes together to result in Θ's, so we should end up with A/Θ. We certainly do, which yields the third isomorphism theorem.

THEOREM 1.13 (THIRD ISOMORPHISM THEOREM) *Let Φ and Θ be congruence relations on A with $\Phi \subseteq \Theta$. Then $(A/\Phi)/(\Theta/\Phi) \cong A/\Theta$.*

Proof of Theorem 1.13. Let $\pi : A \to A/\Theta$ be the canonical epimorphism. Since Θ is the kernel of π and $\Phi \subseteq \Theta$ by hypothesis, π can be injectified to a surjective homomorphism $f : A/\Phi \to A/\Theta$ by Theorem 1.10, sending $\bar{a}_\Phi \to \bar{a}_\Theta$. If $(\bar{a}_\Phi, \bar{b}_\Phi) \in \ker f$, then $\bar{a}_\Theta = \bar{b}_\Theta$, hence $a\Theta b$ which means $(\bar{a}_\Phi, \bar{b}_\Phi) \in \Theta/\Phi$. The converse can be traced easily. Hence, Θ/Φ is the kernel of f, from which it follows that $(A/\Phi)/(\Theta/\Phi) \cong A/\Theta$ by Corollary 1.11. ■

EXERCISES

In general, all maps in the following exercises are homomorphisms.

1. (a) A is a homomorphic image of A.

   (b) If C is a homomorphic image of B and B is a homomorphic image of A, then C is a homomorphic image of A.

2. Consider $p : A \times B \to A$ given by $p(a, b) = a$. What is the kernel of p?

3. Suppose Θ is a congruence relation on A and Φ a congruence relation on B. Describe the kernel of the map $f : A \times B \to A/\Theta \times B/\Phi$ defined by $f(a, b) = (\overline{a}_\Theta, \overline{b}_\Phi)$.

4. If Φ and Θ are congruence relations on A and $f : A \to A/\Phi \times A/\Theta$ is defined by $f(a) = (\overline{a}_\Theta, \overline{a}_\Phi)$, what is the kernel of f?

5. (a) If $f : A \to B$ has kernel Θ, then for every subalgebra C of B, $f^{-1}(C)$ is Θ-invariant. [A subalgebra of A is said to be **saturated** if it's $(\ker f)$-invariant.]

   (b) If $f : A \to B$ is surjective, there exists a bijection between the subalgebras of B and the saturated subalgebras of A.

   (c) Let $\pi : A \to A/\Phi$ be the canonical epimorphism and B a subalgebra of A. Then $B\Phi = \pi^{-1}(\pi(B))$.

6. (a) Every congruence relation on A/Φ is of the form Θ/Φ, with Θ a congruence relation on A containing Φ. For example, $1_{A/\Phi} = \Phi/\Phi$.

   (b) If $\Theta_1/\Phi = \Theta_2/\Phi$ then $\Theta_1 = \Theta_2$.

   (c) There exists a bijection between the congruence relations on A/Φ and the congruence relations on A containing Φ.

7. If $f : A \to B$ is a homomorphism with kernel Θ and Φ is a congruence relation on A such that $\Phi \subseteq \Theta$, the homomorphism $\overline{f} : A/\Phi \to B$ resulting from injectification [Theorem 1.10] has kernel Θ/Φ.

8. If Θ is a congruence relation on B, then $f^{-1}(\Theta) = \{(a_1, a_2) \in A \times A \mid f(a_1)\Theta f(a_2)\}$ is a congruence relation on A containing the kernel of f.

9. An Ω-algebra A is said to be **simple** if $|A| \geq 2$ and the only congruence relations on A are 1_A and $A \times A$. If A is simple, $|B| \geq 2$ and $f : A \to B$ is a surjective homomorphism, then f is an isomorphism.

10. Let B be a subalgebra of A and Φ a congruence relation on A, such that $B\Phi = A$ and $\Phi \cap (B \times B) = 1_B$. [$B$ and Φ are said to be **complementary** in this case.] Assume $\iota : B \hookrightarrow A$ is the canonical monomorphism, and $\pi : A \to A/\Phi$ is the canonical epimorphism.

(a) Every congruence class of Φ contains exactly one element of B. Stated otherwise, the map $f = \pi\iota : B \to A/\Phi$ is bijective, so it's an isomorphism. Conclude that any two subalgebras of A complementary to Φ are isomorphic.

(b) $g = \iota f^{-1} : A/\Phi \to A$ is a homomorphism such that im $g = B$ and $\pi g = 1_{A/\Phi}$. [Such a homomorphism g is said to be a **section**.]

(c) If $g : A/\Phi \to A$ is any homomorphism such that $\pi g = 1_{A/\Phi}$, then im g and Φ are complementary.

(d) $h = f^{-1}\pi : A \to B$ is a homomorphism such that $\ker h = \Phi$ and $h\iota = 1_B$. [Such a homomorphism h is said to be a **retraction**.]

(e) If $h : A \to B$ is any homomorphism such that $h\iota = 1_B$, then B and $\ker h$ are complementary.

(f) Now suppose $e = \iota f^{-1}\pi : A \to A$; show that $e^2 = e$, $\ker e = \Phi$ and im $e = B$. e is said to be **the projection through the congruence relation Φ onto the subalgebra** B.

(g) If $e : A \to A$ is any homomorphism such that $e^2 = e$, im e and $\ker e$ are complementary, and e is the projection through $\ker e$ onto im e.

(h) If G is a group, N a normal subgroup of G corresponding to a congruence relation Φ, and K any subgroup, then K and Φ are complementary if and only if $NK = G$ and $N \cap K = \langle e \rangle$ — so that $G = N \rtimes K$. [*Hint*: Use Exercise 6 of Section 4 to translate the definition of complements.]