Commutative Algebra
Fall 2013, Lecture 1

Karen Yeats
Scribe: Mahdieh Malekian

September 6, 2013

A Bit of Universal Algebra

Definition. Let A be a nonempty set. We define

$$A^0 = \{\varnothing\},$$
$$A^n = \text{set of } n-\text{tuples of elements of } A.$$

An *n-ary function* (or *n-ary operation*) *on* A is a function $A^n \longrightarrow A$, where n is the *arity* of the function.
Note. A 0-ary function just indicates a constant in A.
Definition. A *language* or *type* is a set $\mathcal{F}$ of function symbols each with an associated arity. An *algebra of type* $\mathcal{F}$ is an ordered pair $\mathcal{A} = (A, F)$, where A is a nonempty set and F is a set of functions on A indexed by $\mathcal{F}$ and with matching arities.

An *algebraic structure* is an ordered triple $\mathcal{A} = (A, \mathcal{F}, d)$, where $(A, \mathcal{F})$ is an $\mathcal{F}$ algebra and d is a set of identities using $\mathcal{F}$ and '=' symbol and variable symbols, where we interpret an identity $\alpha(x_1, \ldots, x_n)$ as the sentence $\forall x_1 \forall x_2 \ldots \forall x_n,\ \alpha(x_1, \ldots, x_n)$. So we will have no quantifier except outer $\forall$'s. The *signature* of an algebraic structure or $\mathcal{F}$ algebra is $\mathcal{F}$. (Our book defines it as $(\mathcal{F}, d)$, but then isn't always consistent.)

Example 1 *Groups.*

$$\begin{aligned}(G, (., ^{-1}, 1),\ (x.(y.z) &= (x.y).z,\\ x.x^{-1} &= 1 = x^{-1}.x,\\ x.1 &= 1.x = x)).\end{aligned}$$

And for abelian groups we have:

$$\begin{aligned}(G, (., ^{-1}, 1),\ (x.(y.z) &= (x.y).z,\\ x.x^{-1} &= 1 = x^{-1}.x,\\ x.1 &= 1.x = x,\\ x.y &= y.x))\end{aligned}$$

Example 2 *Rings.*

$$\begin{aligned}(R,(+,.,-,0,1),\ &(R,(+,-,0))\textit{is an abelian group},\\ &x.(y.z)=(x.y).z,\\ &x.1=1.x=x,\\ &x.(y+z)=x.y+x.z,\\ &(y+z).x=y.x+z.x).\end{aligned}$$

Note. Signature does not need to be finite.

Example 3 *Let F be a field. Vector spaces over F are $(V,(+,-,0,(m_\lambda)_{\lambda\in F})$ satisfying $(V,(+,-,0))$ is an abelian group, and where m_λ is scalar multiplication by λ:*

$$\forall\lambda\in F,\ m_\lambda.(x+y)=m_\lambda.x+m_\lambda.y,$$

$$\forall\lambda,\mu\in F,\ m_\lambda(m_\mu(x))=m_{\lambda\mu}(x)\ \textit{and}\ m_\lambda(x)+m_\mu(x)=m_{\lambda+\mu}(x).$$

As usual by abuse of notation the underlying set and the structure will have the same name.

Definition. Let A and B be two $\mathcal{F}$ algebras. Then a function $f:A\longrightarrow B$ is a *homomorphism* if for any n-ary operation $\phi\in\mathcal{F}$,

$$\phi^B(f(a_1),\ldots,f(a_n))=f(\phi^A(a_1,\ldots,a_n))\quad\forall a_1,\ldots,a_n\in A,$$

where ϕ^B means ϕ as interpreted in B.

Let A be an $\mathcal{F}$ algebra. A *substructure* (or a *subalgebra*) of A is a subset of A which is closed under all the operations of the signature.

Note. By their structure, all identities of A hold automatically in a substructure.

An *isomorphism* is a homomorphism which is one-to-one and onto.

In our setup the above requirements for a homomorphism to be an isomorphism are sufficient. If, however, you extend the definitions to allow relations in F as well as functions then you need to require also that the inverse map is a homomorphism.

To see that in our setup the requirements are actually sufficient, suppose f is a homomorphism and a set-bijection. Take $\phi\in\mathcal{F}$, n-ary and $a_1,\ldots,a_n\in A$, $b_1,\ldots,b_n\in B$ such that $f(a_i)=b_i$. Let $g=f^{-1}$, then

$$\begin{aligned}f(\phi^A(g(b_1),\ldots,g(b_n)))&=f(\phi^A(a_1,\ldots,a_n))\\ &=\phi^B(f(a_1),\ldots,f(a_n))\\ &=\phi^B(b_1,\ldots,b_n).\end{aligned}$$

So $\phi^A(g(b_1),\ldots,g(b_n))=g(\phi^B(b_1,\ldots,b_n))$.

Definition. An *embedding* or *monomorphism* is a one-to-one homomorphism. An *epimorphism* is an onto homomorphism.

The next thing we turn to is how to take quotients.

Definition. Let A be an $\mathcal{F}$ algebra, and θ an equivalence relation on A, and suppose for $\forall \phi \in \mathcal{F}$ which is n-ary if $a_1, \ldots, a_n,\ b_1, \ldots, b_n \in A$ with $a_i \theta b_i$,

$$\phi^A(a_1, \ldots, a_n) \theta \phi^A(b_1, \ldots, b_n).$$

Then we say θ is a *congruence* on A.

The point is that the compatibility property in the definition above introduces an $\mathcal{F}$ algebra structure on A/θ as follows

$$\phi^{A/\theta}(a_1/\theta, \ldots, a_n/\theta) = \phi^A(a_1, \ldots, a_n)/\theta,$$

and this is well defined by the property.

Another way to look at the compatibility property is: First view $A \times A$ as an $\mathcal{F}$ algebra coordinatewise, i.e.,

$$\phi^{A \times A}((a_1, b_1), \ldots, (a_n, b_n)) = (\phi^A(a_1, \ldots, a_n), \phi^A(b_1, \ldots, b_n)).$$

Then, if view $\theta \subseteq A \times A$ then the compatibility property says θ is a substructure. Take $(a_i, b_i) \in \theta$ (i.e. $a_i \theta b_i$), then

$$\phi^{\theta \subseteq A \times A}((a_1, b_1), \ldots, (a_n, b_n)) = (\phi^A(a_1, \ldots, a_n), \phi^A(b_1, \ldots, b_n))$$

is in θ iff $\phi^A(a_1, \ldots, a_n) \theta \phi^A(b_1, \ldots, b_n)$. So the compatibility property is equivalent to θ being closed.

Proposition 1 *Let A and B be $\mathcal{F}$ algebras, $f : A \longrightarrow B$ a homomorphism. Let C be a substructure of A then $f(C)$ is a substructure of B. Let D be a substructure of B, then $f^{-1}(D)$ is a substructure of A.*

Proof. Take $\phi \in \mathcal{F}$, which is n-ary, and $a_1, \ldots, a_n \in C$. We have

$$\phi^B(f(a_1), \ldots, f(a_n)) = f(\phi^A(a_1, \ldots, a_n)) \in f(C).$$

For the other part,take $b_1, \ldots, b_n \in D$. For any $a_1, \ldots, a_n$ with $f(a_i) = b_i$ we have

$$\underbrace{\phi^B(b_1, \ldots, b_n)}_{\in D} = f(\underbrace{\phi^A(a_1, \ldots, a_n)}_{\in f^{-1}(D)}).$$

□

Definition. For $f : A \longrightarrow B$ as above we define *kernel* f to be

$$\ker(f) = \{(a, b) \in A^2 : f(a) = f(b)\}.$$

Proposition 2 *For $f : A \longrightarrow B$ as above, $\ker(f)$ is a congruence on A.*

Proof. First note that $\ker(f)$ is a n equivalence relation since '=' is. Now, take $\phi \in \mathcal{F}$, which is an n-ary, and $(a_i, b_i) \in \ker(f), 1 \leq i \leq n$. Then

$$\begin{aligned} f(\phi^A(a_1, \ldots, a_n)) &= \phi^B(f(a_1), \ldots, f(a_n)) \\ &= \phi^B(f(b_1), \ldots, f(b_n)) \\ &= f(\phi^A(b_1, \ldots, b_n)). \end{aligned}$$

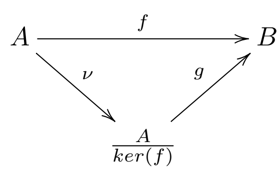
So $(\phi^A(a_1, \ldots, a_n), \phi^A(b_1, \ldots, b_n)) \in \ker(f)$, so $\ker(f)$ is a congruence. □

Therefore, $A/\ker(f)$ makes sense as an object. Further, for any congruence θ we have the natural map

$$\begin{aligned} \nu : &A \longrightarrow A/\theta \\ &a \longmapsto a/\theta, \end{aligned}$$

and this is a homomorphism by definition.

Theorem 1 (First Isomorphism Theorem, universal algebra version) *Let A, B be $\mathcal{F}$ algebras, and $f : A \longrightarrow B$ a homomorphism. Then there is a monomorphism $g : A/\ker(f) \longrightarrow B$ such that*



commutes (i.e. $f = g \circ \nu$), and, in particular, if f is onto then g is an isomorphism.

Proof. Try $g(a/\ker(f)) = f(a)$. If this is well defined then $f = g \circ \nu$. g is indeed well defined, as if a and b are in the same $\ker(f)$ equivalence class, $a/\ker(f) = b/\ker(f)$, or, eqivalently, $(a, b) \in \ker(f)$ or $f(a) = f(b)$. This, also, gives that g is one-to-one.

To check that g is a homomorphism, take $\phi \in \mathcal{F}$ an n-ary, $a_1, \ldots, a_n \in A$, then

$$\begin{aligned} g\left(\phi^{\frac{A}{\ker(f)}}\left(\frac{a_1}{\ker(f)}, \ldots, \frac{a_n}{\ker(f)}\right)\right) &= g\left(\frac{\phi^A(a_1, \ldots, a_n)}{\ker(f)}\right) \\ &= f(\phi^A(a_1, \ldots, a_n)) \\ &= \phi^B(f(a_1), \ldots, f(a_n)) \\ &= \phi^B\left(g\left(\frac{a_1}{\ker(f)}\right), \ldots, g\left(\frac{a_n}{\ker(f)}\right)\right). \end{aligned}$$

□

Definition. Let θ and γ be congruences of A and suppose $\theta \subseteq \gamma$ as subsets of $A \times A$. Then let

$$\frac{\gamma}{\theta} = \left\{ \left(\frac{a}{\theta}, \frac{b}{\theta}\right) \in \left(\frac{A}{\theta}\right)^2 : (a, b) \in \gamma \right\}.$$

Proposition 3 *With θ, γ as above, $\dfrac{\gamma}{\theta}$ is a congruence on $\dfrac{A}{\theta}$.*

Proof. Take $\phi \in \mathcal{F}$, n-ary, and $\left(\dfrac{a_i}{\theta}, \dfrac{b_i}{\theta}\right) \in \dfrac{\gamma}{\theta}$, $1 \leq i \leq n$, then $(a_i, b_i) \in \gamma$ by definition. So

$$(\phi^A(a_1, \ldots, a_n), \phi^A(b_1, \ldots, b_n)) \in \gamma,$$

since γ is a congruence. So

$$\begin{aligned}\left(\phi^{\frac{A}{\theta}}\left(\frac{a_1}{\theta}, \ldots, \frac{a_n}{\theta}\right), \phi^{\frac{A}{\theta}}\left(\frac{b_1}{\theta}, \ldots, \frac{b_n}{\theta}\right)\right) \\ &= \left(\frac{\phi^A(a_1, \ldots, a_n)}{\theta}, \frac{\phi^A(b_1, \ldots, b_n)}{\theta}\right) \\ &\in \frac{\gamma}{\theta}.\end{aligned}$$

□

Theorem 2 (Second Isomorphism Theorem, universal algebra version) *Let A be an $\mathcal{F}$ algebra, $\theta \subseteq \gamma$ congruence on A. Then there is an isomorphism*

$$\frac{\left(\frac{A}{\theta}\right)}{\left(\frac{\gamma}{\theta}\right)} \longrightarrow \frac{A}{\gamma}$$

given by $f\left(\dfrac{\left(\frac{a}{\theta}\right)}{\left(\frac{\gamma}{\theta}\right)}\right) = \frac{a}{\gamma}$.

Proof. Similar to the others. □

The Third Isomorphism Theorem is a bit more technical. For A an $\mathcal{F}$ algebra, θ congruence on A, and B a subset of A, define $B^\theta = \left\{a \in A : B \cap \frac{a}{\theta} \neq \varnothing\right\}$, and $\theta|_B = \theta \cap B^2 = \theta$ restricted to B.

Proposition 4 *B^θ is a substructure of A and $\theta|_B$ is a congruence of B.*

Proof. The second is easy. For the first, take $\phi \in \mathcal{F}$, n-ary, and $a_1, \ldots, a_n \in B^\theta$. Then I can take $b_1, \ldots, b_n \in B$ such that $(a_i, b_i) \in \theta$, so

$$(\phi^A(a_1, \ldots, a_n), \phi^A(b_1, \ldots, b_n)) \in \theta$$

and

$$\phi^A(b_1, \ldots, b_n) = \phi^B(b_1, \ldots, b_n) \in B$$

so $\phi^A(a_1, \ldots, a_n) \in B^\theta$. □

Theorem 3 (Third Isomorphism Theorem, universal algebra version) *Let A be an $\mathcal{F}$ algebra, B its substructure, and θ a congruence of A. Then there is an isomorphism*

$$\frac{B}{(\theta|_B)} \longrightarrow \frac{B^\theta}{(\theta|_{B^\theta})}$$

given by $f\left(\frac{b}{(\theta|_B)}\right) = \frac{b}{(\theta|_{B^\theta})}$.

References

[1] Burris, Sankappanavar, A course in Universal Algebra, www.math.uwaterloo.ca/ snburris/htdocs/ualg.html.