Modern Algebra 2 (MATH 6140)
HANDOUT 2 (September 3, 2008)

ALGEBRA ZERO

By "algebra", we mean a set with operations. Most algebraic investigations require one to restrict attention to algebras that have the same kinds of operations, so the definition of algebra must be preceded by a definition of "language".

Definition 1. (Operation, Signature, Language, Algebra)

(1) For $n \in \mathbb{N}$, an *n-ary operation* on a set A is a function $F\colon A^n \to A$.
(2) (A special case of (1)) An *0-ary operation* on a set A is a function $F\colon A^0 \to A$. Note that, set theoretically, $0 = \emptyset$, so $A^0 = \{\emptyset\}$, and therefore any 0-ary operation $F\colon A^0 \to A$ is really a set of the form $\{(\emptyset, a)\}$ for some $a \in A$. We often say that "$F = a$" rather than "$F = \{(\emptyset, a)\}$".
(3) A *signature* of algebras is a pair $\Sigma := (\mathcal{F}, \sigma)$ where $\mathcal{F}$ is a set (of operation symbols) and $\sigma\colon \mathcal{F} \to \mathbb{N}$ is a function (assigning arity). σ is called the *signature function*. (Sometimes what we call a signature is called a *language*, but we reserve the word 'language' for the set $\mathcal{L}$ of "formulas" in a given signature. Either way, choosing a signature is the same as chossing a language.)
(4) An *algebra* of signature $(\mathcal{F}, \sigma)$ is an ordered pair $\mathbf{A} = \langle A; \mathcal{F}^{\mathbf{A}} \rangle$ where A is a set and $\mathcal{F}^{\mathbf{A}} = \{F^{\mathbf{A}} \mid F \in \mathcal{F}\}$, where $F^{\mathbf{A}}\colon A^{\sigma(F)} \to A$ is an operation on A.

We are usually not so formal, and may write $G = \langle G; \cdot, {}^{-1}, 1 \rangle$ and say in words that $\cdot$ is a binary operation, ${}^{-1}$ is a unary operation and 1 is a 0-ary operation. (Note that the bold face font on the algebra symbol G has been omitted and the operations are simply listed rather than described as a set.) But to formalize this we take $\mathcal{F} = \{\cdot, {}^{-1}, 1\}$, specify the signature by saying that $\sigma(\cdot) = 2$, $\sigma({}^{-1}) = 1$, and $\sigma(1) = 0$, and write $\mathbf{G} = \langle G; \mathcal{F}^{\mathbf{G}} \rangle$.

Example 2. (Algebras in their usual signatures)
Semigroups: $\langle S; \cdot \rangle$, Monoids: $\langle M; \cdot, 1 \rangle$, Groups: $\langle G; \cdot, {}^{-1}, 1 \rangle$,
G-sets: $\langle X; \{g(x) \mid g \in G\} \rangle$, Rings: $\langle R; \cdot, +, -, 0, 1 \rangle$,
$\mathbb{F}$-vector spaces: $\langle V; +.-, 0, \{\alpha(x) \mid \alpha \in \mathbb{F}\} \rangle$,
$\mathbf{R}$-modules: $\langle M; +.-, 0, \{r(x) \mid r \in \mathbf{R}\} \rangle$, Lattices: $\langle L; \vee, \wedge \rangle$.

There are natural generalizations of the algebra concept:

(1) Partial algebras: same as above, but operations are allowed to be partial. A *n-ary partial operation* on A is a function $P\colon D \to A$ where $D \subseteq A^n$. (E.g. the inverse operation of a field is a partial unary operation.)
(2) Infinitary algebras: same as above, but operations are allowed to be infinitary. A *κ-ary operation* on A is a function $I\colon A^\kappa \to A$, where κ is a cardinal. (E.g. a complete lattice has κ-ary join and meet operations for every κ.)

(3) Multisorted algebras: Same as above, but multiple universes (or *sorts*) are allowed. (E.g. a G-set X may be defined as a 2-sorted algebra $\langle X, G; \circ, \cdot, ^{-1}, 1\rangle$ with one sort for elements of X, another sort for group elements, and operations that allow us to express the action, $\circ\colon G \times X \to X$, and to express that $\langle G; \cdot, ^{-1}, 1\rangle$ is a group.)
(4) Hyperalgebras: defined like algebras, but operations can be multivalued. These structures are models of nondeterministic computation. It is possible to think of ordered sets as hyperalgebras: if $\langle P; \leq\rangle$ is an ordered set, then $\leq$ can be thought of as a unary hyperoperation. Any $x \in P$ is mapped by $\leq$ to the set of all related $y \in P$; i.e., $\leq(x) = \{y \in P \mid y \leq x\}$.

Homomorphisms.

Definition 3. Let $\mathcal{L}$ be a language and let $\mathbf{A}, \mathbf{A}_i$ and $\mathbf{B}$ be $\mathcal{L}$-algebras.

(1) A relation $R \subseteq A_1 \times \cdots \times A_k$ between the $\mathbf{A}_i$ is *compatible* if whenever $r_1, \ldots, r_n \in R$ and F is an n-ary $\mathcal{L}$-operation, then $F(r_1, \ldots, r_n) \in R$.
(2) A *homomorphism* from $\mathbf{A}$ to $\mathbf{B}$ is a function $\varphi\colon A \to B$ whose graph is a compatible relation between $\mathbf{A}$ and $\mathbf{B}$. Explicitly, this compatibility means
$$\varphi(F^{\mathbf{A}}(a_1, \ldots, a_n)) = F^{\mathbf{B}}(\varphi(a_1), \ldots, \varphi(a_n))$$
holds for every F in this language.
(3) The *kernel* of a homomorphism $\varphi\colon \mathbf{A} \to \mathbf{B}$ is the kernel of φ considered as a set function.
(4) A compatible equivalence relation is a *congruence*. Explicitly, the statement that an equivalence relation θ on $\mathbf{A}$ is compatible is the statement that for every $a_i, b_i \in A$ and every operation F, if $a_i \equiv b_i \pmod{\theta}$ for all i, then $F(a_1, \ldots, a_n) \equiv F(b_1, \ldots, b_n) \pmod{\theta}$. This turns out to be equivalent to the property that θ is compatible with all *basic translations*, which are functions of the form $\beta(x) = F(c_1, \ldots, c_{i-1}, x, d_{i+1}, \ldots, d_n)$. Thus an equivalence relation θ is a congruence iff $a \equiv b \pmod{\theta} \implies \beta(a) \equiv \beta(b) \pmod{\theta}$ for all basic translations β.

Facts 4. Let $\varphi\colon \mathbf{A} \to \mathbf{B}$ be a homomorphism of $\mathcal{L}$-algebras and let θ be a congruence on $\mathbf{A}$.

(1) $\ker(\varphi)$ is a congruence.
(2) There is a well-defined $\mathcal{L}$-algebra structure on A/θ, namely for an operation F define $F(a_1/\theta, \ldots, a_n/\theta) = F(a_1, \ldots, a_n)/\theta$. This algebra is the *quotient modulo* θ, and is written $\mathbf{A}/\theta$.
(3) The $\mathcal{L}$-algebra structure on A/θ from (2) is the unique $\mathcal{L}$-algebra structure on this set that makes the natural map $\nu\colon \mathbf{A} \to \mathbf{A}/\theta$ a homomorphism.
(4) If $\mathbf{S} \leq \mathbf{A}$ is a subalgebra, then $\mathbf{S}^\theta$ is also a subalgebra.

The Isomorphism Theorems.

First Isomorphism Theorem. If $\varphi\colon \mathbf{A} \to \mathbf{B}$ is a homomorphism, then there is a unique isomorphism $\overline{\varphi}\colon \mathbf{A}/\ker(\varphi) \to \mathrm{im}(\varphi)$ such that $\overline{\varphi} \circ \nu = \varphi$.

Second Isomorphism Theorem. If $\mathbf{S} \leq \mathbf{A}$ and θ is a congruence on $\mathbf{A}$, then the inclusion map $\mathbf{S} \subseteq \mathbf{S}^\theta$ induces an isomorphism $\mathbf{S}/(\theta|_S) \to \mathbf{S}^\theta/(\theta|_{S^\theta})$.

Third Isomorphism Theorem. If $\theta \subseteq \psi$ are congruences on $\mathbf{A}$, then the function $a/\theta \mapsto a/\psi$ is a surjective homomorphism from $\mathbf{A}/\theta$ to $\mathbf{A}/\psi$ whose kernel is ψ/θ. (Thus $(\mathbf{A}/\theta)/(\psi/\theta) \cong \mathbf{A}/\psi$.)

Remark. There is a useful statement that is equivalent to the conjunction of the First and Third Isomorphism Theorems, it is: If $\varphi\colon \mathbf{A} \to \mathbf{B}$ is a homomorphism, and $\theta \subseteq \ker(\varphi)$, then there is a unique homomorphism $\overline{\varphi}\colon \mathbf{A}/\theta \to \mathbf{B}$ such that $\overline{\varphi} \circ \nu = \varphi$. Moreover $\mathrm{im}(\overline{\varphi}) = \mathrm{im}(\varphi)$ and $\ker(\overline{\varphi}) = \ker(\varphi)/\theta$.

The following has been called the "Fourth Isomorphism Theorem".

Correspondence Theorem. If θ is a congruence on $\mathbf{A}$, then the map $\psi \mapsto \psi/\theta$ is an isomorphism from the lattice of congruences of $\mathbf{A}$ extending θ and the lattice of congruences of $\mathbf{A}/\theta$. The map $\mathbf{S} \mapsto \mathbf{S}/\theta$ is an isomorphism from the lattice of θ-saturated subalgebras of $\mathbf{A}$ to the lattice of subalgebras of $\mathbf{A}/\theta$.

Algebras with underlying group structure.

Some of the above may seem foreign if you have only considered algebras with underlying group structure, like groups, rings or vector spaces, where kernels are identified with normal subgroups. In fact, the concept of a normal subgroup of a group is nothing other than an abbreviation of the concept of a congruence.

Let $\mathbf{A} = \langle A; \cdot, {}^{-1}, 1, F_1, F_2, \ldots\rangle$ be an algebra with underlying group structure, and let $G := \langle A; \cdot, {}^{-1}, 1\rangle$ be the underlying "pure" group. If θ is a congruence on $\mathbf{A}$, then it is also a congruence on G. The θ-class $N = 1/\theta$ is the θ-saturation of $S = \{1\}$, which is a subgroup of G, hence $N = \mathbf{S}^\theta$ is also a subgroup of G. Moreover, $a \equiv b \pmod{\theta}$ iff $ab^{-1} \equiv 1 \pmod{\theta}$ iff $ab^{-1} \in N$. Since θ is a congruence, it is preserved by all basic translations $\beta(x) = F(c_1, \ldots, c_{i-1}, x, d_{i+1}, \ldots, d_n) = F(\mathbf{c}, x, \mathbf{d})$, hence

$$\begin{aligned} ab^{-1} \in N &\Leftrightarrow a \equiv b \pmod{\theta} \\ &\Rightarrow \beta(a) \equiv \beta(b) \pmod{\theta} \\ &\Leftrightarrow \beta(a)\beta(b)^{-1} \in N \\ &\Leftrightarrow F(\mathbf{c}, a, \mathbf{d}) \cdot F(\mathbf{c}, b, \mathbf{d})^{-1} \in N. \end{aligned}$$

Thus, if the subgroup $N \leq G$ is a congruence class of 1, then

$$ab^{-1} \in N \Rightarrow F(\mathbf{c}, a, \mathbf{d}) \cdot F(\mathbf{c}, b, \mathbf{d})^{-1} \in N \tag{0.1}$$

for all operations F and all $c_i, d_j \in A$. Conversely, if N is a subgroup of G satisfying implication (0.1), then the equivalence relation on A defined by "$a \equiv b \pmod{\theta}$ iff $ab^{-1} \in N$" is preserved by all basic translations, hence is a congruence on $\mathbf{A}$. This shows that any congruence θ on $\mathbf{A}$ can be "abbreviated" by the subgroup $N = 1/\theta$, which is simply an arbitrary subgroup of G satisfying the "normality condition" (0.1).

Exercises 5.

(1) Show that if $\mathbf{A} = \langle A; \cdot, {}^{-1}, 1\rangle$ is a pure group, then a subgroup N satisfies condition (0.1) iff it is a normal subgroup. (Hint: the basic translations have the form $\beta(x) = cx, xd, x^{-1}$, or 1.)

(2) What is the correct abbreviation of "congruence" for a group with a group of automorphisms adjoined as new unary operations?

(3) Show that if $\mathbf{A}$ is a ring, then a subgroup N satisfies condition (0.1) iff it is an ideal.

(4) What is the correct abbreviation of "congruence" for a ring with nonassociative (but still distributive) multiplication?

(5) What is the correct abbreviation of "congruence" for a ring with nonassociative and nondistributive multiplication?