Modern Algebra 2 (MATH 6140)
HANDOUT 2 (January 30, 2008)

FREE ALGEBRAS

Our definition of "free" will make use of the vague notion of a "class of structures" in order to point out the existence of free topological spaces and free ordered sets, as well as free algebras. This vague notion is made precise when we later define "concrete category", but for these notes it suffices to think of a class of structures as a class of objects where each has an underlying set and for which certain set-maps between them are called "morphisms".

Definition 1. (Free objects) Let $\mathcal{C}$ be a class of structures and let X be a set. A structure $\mathbf{F} = \mathbf{F}_{\mathcal{C}}(X)$ is *free over X relative to $\mathcal{C}$* if

(1) $X \subseteq F$,
(2) $\mathbf{F} \in \mathcal{C}$, and
(3) (Universal property) For every $\mathbf{A} \in \mathcal{C}$ and every set-map $f\colon X \to A$ there is a unique morphism $\overline{f}\colon \mathbf{F} \to \mathbf{A}$ such that $\overline{f}|_X = f$.

Example 2.
(1) X equipped with the discrete topology is free over X relative to the class of topological spaces with continuous maps.
(2) X equipped with the discrete order is free over X relative to the class of ordered sets with monotone maps.
(3) Every $\mathbb{D}$-vector space is free over a vector space basis relative to the class of all $\mathbb{D}$-vector spaces with linear transformations.
(4) The polynomial ring $\mathbb{Z}[x_1, \ldots, x_n]$ is free over $X = \{x_1, \ldots, x_n\}$ relative to the class of commutative rings and homomorphisms.
(5) The $\mathbf{R}$-module $\oplus_{x \in X}\mathbf{R}$ is free over X relative to the class of all $\mathbf{R}$-modules with homomorphisms.

Although free objects exist in some classes of structures that are not classes of algebras, they are more important in algebra for the following reason. Suppose that $\mathbf{A} \in \mathcal{C}$ and that X is a set that is at least as large as A. If $\mathbf{F} = \mathbf{F}_{\mathcal{C}}(X)$ exists, then any surjective map $f\colon X \to A$ can be extended to a surjective morphism $\overline{f}\colon \mathbf{F} \to \mathbf{A}$. If an analogue of the first isomorphism theorem holds for our structures, then there is an induced bijective morphism $\overline{\overline{f}}\colon \mathbf{F}/\theta \to \mathbf{A}$. In general, this is not very interesting; for example, when we are dealing with topological spaces we only learn that there is a bijective continous map $\overline{\overline{f}}\colon \mathbf{F}/\theta \to \mathbf{A}$ from the discrete space $\mathbf{F}/\theta$ to $\mathbf{A}$. This yields no information about $\mathbf{A}$ except its cardinality. But bijective homomorphisms of algebras are isomorphisms, which means that we have described $\mathbf{A}$ up to isomorphism as a quotient of a free algebra. Thus, a typical algebra $\mathbf{A} \in \mathcal{C}$ can be described in a convenient way as $\mathbf{F}/\theta$, or more simply as a pair $\langle X \mid R \rangle$ where X is a generating

set for $\mathbf{F} = \mathbf{F}_{\mathcal{C}}(X)$ and R is a generating set for a congruence $\theta = \theta(R)$. The symbol $\langle X \mid R \rangle$ then represents $\mathbf{F}_{\mathcal{C}}(X)/\theta(R)$ ($\cong \mathbf{A}$).

Our next goal is to characterize free algebras as algebras that have an independent generating set. For this we need to know what "independent" and "generating set" mean.

Generation

Definition 3. (Closure operator) Let X be a set and let $\mathcal{P}(X)$ be the collection of all subsets of X. A *closure operator* on X is a function $\mathsf{cl} : \mathcal{P}(X) \to \mathcal{P}(X)$ that is

(i) Extensive: $U \subseteq \mathsf{cl}(U)$,
(ii) Idempotent: $\mathsf{cl}(\mathsf{cl}(U)) = \mathsf{cl}(U)$, and
(iii) Isotone: $U \subseteq V \Longrightarrow \mathsf{cl}(U) \subseteq \mathsf{cl}(V)$.

A subset $U \subseteq X$ is *closed* if $U = \mathsf{cl}(U)$. The closed set *generated* by U is $\langle U \rangle := \mathsf{cl}(U)$. A closed set C is *finitely generated* if $C = \mathsf{cl}(U)$ for some finite U, and is *cyclic* (or *principal*) if $C = \mathsf{cl}(\{u\})$ for some $u \in X$.

Exercises.

(1) Show that the collection of closed sets of a closure operator is closed under arbitrary intersection.
(2) Show conversely that any collection of subsets of X that is closed under arbitrary intersection is the collection of closed subsets of some closure operator.

The examples of importance to us are the closure operators of subuniverse generation and congruence generation. If $\mathbf{A}$ is an algebra, write $\langle X \rangle$ or $\mathrm{Sg}^{\mathbf{A}}(X)$ for the subuniverse generated by the subset $X \subseteq A$, and $\theta(R)$ or $\mathrm{Cg}^{\mathbf{A}}(R)$ for the congruence generated by the pairs $R \subseteq A \times A$. (Check that these are closure operators.)

Exercises.

(3) Show that *equalizer* of two homomorphisms $\alpha, \beta \colon \mathbf{A} \to \mathbf{B}$ is a subuniverse. (The equalizer of α and β is $\{x \in A \mid \alpha(x) = \beta(x)\} = \pi_1(\alpha \cap \beta)$.) Conclude that if two homomorphisms agree on a generating set, then they are equal.
(4) Show that if a homomorphism $\varphi \colon \mathbf{A} \to \mathbf{B}$ contains a generating set for $\mathbf{B}$ in its image, then φ is surjective.

Definition 4. (Terms) Let $\mathcal{L} = (\mathcal{F}, \sigma)$ be a language. The *set of $\mathcal{L}$-terms* is the smallest set T such that

(i) $x_i \in T$ for $i \in \omega$ and $c \in T$ for all $c \in \mathcal{F}$ of arity zero, and
(ii) If $t_1, \ldots, t_n \in T$ and $F \in \mathcal{F}$ is n-ary, then $F(t_1, \ldots, t_n) \in T$.

An *$\mathcal{L}$-term* is an element of T.

For any $\mathcal{L}$-algebra, each operation symbol F has an interpretation as a concrete operation $F^{\mathbf{A}}$. Inductively we can interpret each term t as a concrete operation $t^{\mathbf{A}}$. (I will usually omit these kinds of superscripts, as in, e.g., the following theorem.)

Theorem 5. (Subuniverse generation) *If* $\mathbf{A}$ *is an* $\mathcal{L}$*-algebra and* $G \subseteq A$*, then* $a \in \langle G \rangle$ *iff there is a term* t *and distinct* $g_1, \ldots, g_n \in G$ *such that* $a = t(g_1, \ldots, g_n)$*.*

Sketch of proof. First show by induction on complexity of terms that any subuniverse containing G also contains every element of the form $t(g_1, \ldots, g_n)$. Then observe that the set of these elements is a subuniverse, hence is $\langle G \rangle$. □

Independence

Definition 6. (Dependence relations, independence, basis) A *dependence relation* is a pair of $\mathcal{L}$-terms, either denoted (s, t) or $s = t$. If $\mathbf{A}$ is an $\mathcal{L}$-algebra, then a tuple $(a_1, \ldots, a_n) \in A^n$ *satisfies* $s = t$ if $s(a_1, \ldots, a_n) = t(a_1, \ldots, a_n)$ holds.

Let $\mathcal{C}$ be a class of $\mathcal{L}$-algebras. A dependence relation is *trivial* relative to $\mathcal{C}$ if it is satisfied by every tuple of every algebra in $\mathcal{C}$, otherwise it is *nontrivial*.

A tuple in some $\mathbf{A} \in \mathcal{C}$ is *independent* relative to $\mathcal{C}$ if it satisfies no nontrivial dependence relation. A subset $X \subseteq A$ is independent relative to $\mathcal{C}$ if any tuple of distinct elements from X is independent.

A *basis* for $\mathbf{A}$ relative to $\mathcal{C}$ is an independent generating set.

Theorem 7. (Characterization of free algebras) *Assume that* $\mathcal{C}$ *is closed under the formation of subalgebras. If* $\mathbf{F} \in \mathcal{C}$ *and* $X \subseteq F$*, then* $\mathbf{F}$ *is free over* X *relative to* $\mathcal{C}$ *iff* X *is a basis for* $\mathbf{F}$ *relative to* $\mathcal{C}$*.*

Sketch of proof. Assume $\mathbf{F}$ is free over X relative to $\mathcal{C}$. If X were not independent relative to $\mathcal{C}$, then there would exist a tuple $\mathbf{x}$ of distinct elements of X satisfying a nontrivial dependence relation $s = t$. The nontriviality means that there is an $\mathbf{A} \in \mathcal{C}$ containing a tuple $\mathbf{a}$ such that $s(\mathbf{a}) \neq t(\mathbf{a})$. Choose an arbitrary function $f\colon X \to A$ satisfying $f(\mathbf{x}) = \mathbf{a}$, which is possible since the components of $\mathbf{x}$ are distinct. This function cannot be extended to a homomorphism $\overline{f}\colon \mathbf{F} \to \mathbf{A}$, since then $s(\mathbf{a}) = s(f(\mathbf{x})) = s(\overline{f}(\mathbf{x})) = \overline{f}(s(\mathbf{x})) = \overline{f}(t(\mathbf{x})) = t(\mathbf{a})$, contrary to $s(\mathbf{a}) \neq t(\mathbf{a})$. This contradiction shows that X is independent.

Let $\mathbf{G} = \langle X \rangle \in \mathcal{C}$ be the subalgebra of $\mathbf{F}$ that is generated by X. By the freeness of $\mathbf{F}$, the identity function on X can be extended to a homomorphism $\overline{f}\colon \mathbf{F} \to \mathbf{G}$. Composing with $\subseteq\colon \mathbf{G} \to \mathbf{F}$ we get a homomorphism $\varphi = \subseteq \circ \overline{f}\colon \mathbf{F} \to \mathbf{F}$ that is the identity on X. But the identity on $\mathbf{F}$ is the *unique* extension of $\subseteq\colon X \to F$ to an algebra homomorphism, so $\mathrm{id} = \varphi = \subseteq \circ \overline{f}$. Since φ is surjective, so is $\subseteq$, hence $\mathbf{G} = \mathbf{F}$, hence X generates $\mathbf{F}$.

Conversely, assume that X is a basis for $\mathbf{F}$ relative to $\mathcal{C}$. For any $\mathbf{A} \in \mathcal{C}$ and any function $f\colon X \to A$, we use Theorem 5 to extend this function to a homomorphism $\overline{f}\colon \mathbf{F} \to \mathbf{A}$. Namely, represent a given $a \in F$ as $a = t^{\mathbf{F}}(g_1, \ldots, g_n)$ for some term t and some generating elements $g_i \in X$. Then define $\overline{f}(a) = t^{\mathbf{A}}(f(g_1), \ldots, f(g_n))$. It is straightforward to check that, if $\overline{f}$ is a well-defined function, then it is a homomorphism extending f. But $\overline{f}$ can only fail to be well-defined if there is an $a \in F$ with two representations $a = s^{\mathbf{F}}(\mathbf{g}) = t^{\mathbf{F}}(\mathbf{g})$ while $s^{\mathbf{A}}(f(\mathbf{g})) \neq t^{\mathbf{A}}(f(\mathbf{g}))$. If this happened,

then $\mathbf{g}$ would be a tuple of distinct elements of X satisfying a dependence relation $s = t$, which is nontrivial since it is not satisfied by some other tuple $f(\mathbf{g})$ from some member of $\mathcal{C}$. This contradicts the independence of X. □

Definition 8. An *identity* is a dependence relation, considered as a first-order formula. A *variety* is a class of algebras definable by identities.

It is a theorem of Birkhoff that a class of algebras is a variety iff it is closed under the formation of homomorphic images, subalgebras and products. A class closed under isomorphic images, subalgebras and products is called a *prevariety*. Every variety is a prevariety, but not conversely (e.g., the prevariety of torsion-free groups is not a variety).

Existence and uniqueness of free algebras

Theorem 9. (Existence of free algebras) *If $\mathcal{P}$ is a prevariety, then $\mathcal{P}$ contains free algebras over any set X.*

Proof. It is enough to construct an algebra in $\mathcal{P}$ that is free over some set Y of size $|X|$, for then we may replace it by an isomorphic algebra where Y corresponds to X under the isomorphism. In fact, it is enough to construct an algebra in $\mathcal{P}$ that has an independent set Y of size $|X|$, since by Theorem 7 the subalgebra generated by Y will be free. So this is what we do.

Let I be an index set of size $|X|$. Consider the collection of all pairs $(\mathbf{A}, \mathbf{a})$ where $\mathbf{A} \in \mathcal{P}$ and $\mathbf{a}$ is an I-tuple of elements of A. Our goal is to locate such a pair where $\mathbf{a}$ is an indexing of an independent subset of $\mathbf{A}$. To this end, let Γ be the set of all sequences $\gamma = (s, t; i_1, \ldots, i_n)$ where $s(x_1, \ldots, x_n) = t(x_1, \ldots, x_n)$ is a nontrivial dependence relation and $(i_1, \ldots, i_n)$ is an n-tuple of elements of I. For each $\gamma \in \Gamma$ choose a pair $(\mathbf{A}, \mathbf{a})_\gamma$ such that $s(a_{i_1}, \ldots, a_{i_n}) \neq t(a_{i_1}, \ldots, a_{i_n})$. (This is possible: $s = t$ is nontrivial, so some n-tuple of elements in some $\mathbf{A} \in \mathcal{P}$ falsifies $s = t$. Put those elements in the $(i_1, \ldots, i_n)$ positions of an I-tuple and choose the other coordinates of the tuple randomly.)

Now, consider the product object $\prod_{\gamma\in\Gamma}(\mathbf{A}, \mathbf{a})_\gamma$. This is a pair $(\mathbf{F}, \mathbf{x})$ where $\mathbf{F} = \prod_{\gamma\in\Gamma} \mathbf{A}_\gamma \in \mathcal{P}$ and $\mathbf{x}$ is the I-tuple of elements of F whose i-th coordinate is the Γ-tuple of i-th coordinates of the $\mathbf{a}_\gamma$'s. Now, for any $\gamma = (s, t; i_1, \ldots, i_n)$ we get that the dependence relation $s(x_{i_1}, \ldots, x_{i_n}) = t(x_{i_1}, \ldots, x_{i_n})$ fails in coordinate γ of $\mathbf{x}$. Thus, $\mathbf{x}$ is an indexing of an independent subset of $\mathbf{F}$ of size $|X|$. □

Theorem 10. (Uniqueness of free algebras) *Any bijection $f\colon X \to Y$ extends in a unique way to an isomorphism $\overline{f}\colon \mathbf{F}_\mathcal{C}(X) \to \mathbf{F}_\mathcal{C}(Y)$.*

Proof. A bijection $f\colon X \to Y$ is a function $f\colon X \to F_\mathcal{C}(Y)$, hence can be extended in a unique way to a homomorphism $\overline{f}\colon \mathbf{F}_\mathcal{C}(X) \to \mathbf{F}_\mathcal{C}(Y)$. Similarly $f^{-1}\colon Y \to X$ can be extended in a unique way to a homomorphism $\overline{f^{-1}}\colon \mathbf{F}_\mathcal{C}(Y) \to \mathbf{F}_\mathcal{C}(X)$. Now $\overline{f^{-1}} \circ \overline{f}\colon \mathbf{F}_\mathcal{C}(X) \to \mathbf{F}_\mathcal{C}(X)$ is a homomorphism that is the identity on X. According to the

universal property of free algebras, the identity function is the unique homomorphism with this property. Thus $\overline{f^{-1}} \circ \overline{f} = \mathrm{id}$, and by a similar argument $\overline{f} \circ \overline{f^{-1}} = \mathrm{id}$, so $\overline{f}$ is an isomorphism. □

The proof of the following result is given at the bottom of the first page of these notes.

Theorem 11. *Every algebra in a prevariety $\mathcal{P}$ is a homomorphic image of a free algebra in $\mathcal{P}$.*

Presentations and their universal property

By Theorem 11, if $\mathcal{P}$ is a (pre)variety, then every $\mathbf{A}$ is isomorphic to $\mathbf{F}/\theta$ where $\mathbf{F}$ is freely generated by some set G and θ is a congruence (generated, say, by some set of pairs R). Thus the pair $\langle G \mid R \rangle$ contains all the date necessary to describe $\mathbf{A}$ up to isomorphism.

Definition 12. (Presentations relative to varieties) A *presentation* of $\mathbf{A}$ by generators and relations, relative to a variety $\mathcal{V}$, is a pair $\langle G \mid R \rangle$ such that $\mathbf{A} \cong \mathbf{F}_{\mathcal{V}}(G)/\theta(R)$.

In this definition we have specialized from prevarieties to varieties to guarantee that $\mathbf{F}_{\mathcal{V}}(G)/\theta(R) \in \mathcal{V}$ for any G and R.

Example 13.
(1) An algebra is free over G iff it has $\langle G \mid \emptyset \rangle$ for a presentation.
(2) The group $\mathbb{Z}_n$ has a (multiplicative) presentation $\langle a \mid a^n = 1 \rangle$ relative to the variety of groups. It has other presentations as well, like $\langle a, b \mid a^n = 1 = b^n = b^{n+1} \rangle$
(3) Describing the ring $\mathbb{Z}[\sqrt{5}]$ as $\mathbb{Z}[x]/(x^2-5)$ is essentially the same thing as describing it with the presentation $\langle x \mid x^2 = 5 \rangle$ relative to the variety of rings.
(4) Later we will learn an algorithm to decide the isomorphism type of an abelian group from a presentation. Can you determine now the isomorphism type of $\langle x, y, z \mid 3x + 3y + 9z = 0 \rangle$?

It is possible to couple the universal property of free algebras with the isomorphism theorems to produce a universal property for presentations.

Theorem 14. (Universal property for presentations) *If $\mathbf{P} = \langle G \mid R \rangle$ relative to a variety $\mathcal{V}$, then $\mathbf{P}$ is generated by G, satisfies the relations in R, and for any $\mathbf{A} \in \mathcal{V}$ and any set-map $f \colon G \to A$ such that $f(G)$ satisfies relations obtained from those in R by replacing each $g \in G$ by $f(g)$, then f extends uniquely to a homomorphism $\overline{f} \colon \mathbf{P} \to \mathbf{A}$.*

For example, the group $\mathbb{Z} \times \mathbb{Z}$ is presented by $\langle x, y \mid xy = yx \rangle$. Thus, if $\mathbf{A}$ is any group and $a, b \in A$ are elements that commute, then there is a unique group homomorphism $\overline{f} \colon \mathbb{Z} \times \mathbb{Z} \to \mathbf{A} \colon x \mapsto a, y \mapsto b$.