Lecture 1. Monoids: General algebraic aspects

Definition. A monoid is a set equipped with and associative binary operation that has an identity element.

Given a monoid M, we have the following data:

i) a set $|M|$;
ii) a map $*_M : |M| \times |M| \to |M|; (x, y) \mapsto x *_M y$, satisfying $(x *_M y) *_M z = x *_M (y *_M z)$ for all $x, y, z \in |M|$;
iii) an element $e_M \in |M|$, satisfying $x *_M e_M = x = e_M *_M x$ for all $x \in |M|$.

Often we take liberties with the notation, using the name M to refer to the set $|M|$ or suppressing the subscript on e or on $*$.

Definition. A *submonoid* of M is a subset that: *i)* contains e, and *ii)* contains $x * y$ whenever it contains x and y. Given a subset $X \subseteq M$, the *submonoid generated by* X, denoted $\langle X \rangle_M$, is the intersection of all submonoids of M that contain X. We say M is *finitely generated* if there is a finite subset of M that generates M, *i.e.*, that is contained in no proper submonoid of M.

Definition. Given monoids M_α, $\alpha \in A$, the *product* $\prod M_\alpha$ the set of functions $x : A \to \cup M_\alpha; \alpha \mapsto x_\alpha$, with $x_\alpha \in M_\alpha$, where we define $x * y$ by $(x * y)_\alpha = x_\alpha * y_\alpha$. (The product of a pair of monoids, M and N is denoted $M \times N$.)

Definition. A *congruence* on a monoid M is a submonoid of $M \times M$ that is also an equivalence relation on M. If C is a congruence on M, then the set of equivalence classes is denoted M/C.

1.1. Fact. Given any subset $\Gamma \subseteq M \times M$, there is a smallest congruence containing Γ, namely

$$\langle\langle \Gamma \rangle\rangle := \bigcap \{\, C \mid C \supseteq \Gamma \text{ and } C \text{ is a congruence} \,\}.$$

1.2. Exercise. Let C be a congruence on M. Let $[x]$ denote the equivalence class of $x \in M$.

1) If $(x, x') \in C$ and $(y, y') \in C$, then by assumption, $(x * y, x' * y') \in C$, hence $[x * y] = [x' * y']$.
2) By 1), $[x] * [y] := [x * y]$ determines a well-defined operation on M/C.
3) Moreover, M/C is a monoid with respect to this operation.

Definition. Let L and M be monoids. A function $\phi : L \to M$ is called a *(monoid) morphism* if *i)* $\phi(e_L) = e_M$, and *ii)* $\phi(x *_L y) = \phi(x) *_M \phi(y)$ for all $x, y \in L$.

1.3. Exercise. Let $\phi : L \to M$ be a morphism. Let $C := \{\, (x, y) \in L \times L \mid \phi(x) = \phi(y) \,\}$. Then C is a congruence on L, and ϕ can be written as the composition $\phi = \iota \circ \pi$, where

$\pi : L \to L/C; x \mapsto [x]$ and $\iota : L/C \to M; [x] \mapsto \phi(x)$. Moreover, ι is an injective morphism and π is a surjective morphism.

1.4. Fact. Any group is a monoid, any group homomorphism is a monoid morphism, and any monoid morphism between groups is actually a group homomorphism. More formally, the category of groups is a full subcategory of the category of monoids.

1.5. Fact. With any monoid M we can associate a group $G(M)$ and a monoid morphism $\gamma_M : M \to G(M)$ with the following universal mapping property: given any monoid morphism $\phi : M \to H$ with H a group, there is a unique group homomorphism $\overline{\phi} : G(M) \to H$ such that $\overline{\phi} \circ \gamma_M = \phi$.

Sketch of proof. Let F be the free group on $|M|$. Any finite sequence $u = (u_1, \ldots, u_n)$ of elements of $|M|$ determines an element $u_F := u_1 \cdot u_2 \cdots u_n \in F$ and an element $u_M := u_1 *_M u_2 \cdots *_M u_n \in M$. Let N be the ideal of F generated by the set

$$\{\, u_F \cdot {v_F}^{-1} \mid u_M = v_M \,\},$$

where u and v range over all finite sequences of elements of $|M|$. One can show that the composition $M \to F \to F/N$ is a monoid morphism. Moreover, one can also show that this morphism has the universal mapping property specified for γ_M. Indeed, $\phi : M \to H$ considered merely as a map fo sets induces a group homomorphism $\hat{\phi} : F \to H$, and one can show that $N \subseteq \ker \hat{\phi}$. Hence, $\hat{\phi}$ induces a group homomorphism $\overline{\phi} : F/N \to H$.

1.6. Exercise. Provide the details in the sketch.

1.7. Exercise. Show that $G(M)$ is commutative if M is.

Problem. Find (interesting) necessary and/or sufficient conditions for γ_M to be injective.
Comment. This problem is discussed at length in Chapter 12 (Volume II) of [CP].

References

[CP] A. H. Clifford & G. B. Preston, *The Algebraic Theory of Semigroups*, AMS 1967.