Chevalley, Claude. (1956). *Fundamental Concepts of Algebra*. New York: Academic Press.
https://github.com/kmi-ne/Math-MyNotes

Chapter 1

Monoids

1.1 Definition of a monoid
結合的かつ中立元を持つ→モノイド．一般結合定理．可換モノイドと一般可換定理．
1.2 Submonoids. Generators
…

1.1 Definition of a monoid

Convention 1.1

1. Syn. for $\top$ —
$$+\ /\ \cdot$$
2. Syn. for $\top(a,b)$ —
$$a \top b$$
3. Syn. for $a \cdot b$ —
$$ab$$

Definition 1.2 — Underlying set

$$\underline{\top} := \mathrm{img}(\mathrm{dom}(\top))$$

— label: `dfn_uds`

$$(\top\colon A \times A \to A) \to \underline{\top} = A$$

Definition 1.3 — $\top$ is an (internal) law of composition

$$\mathsf{LawComp}(\top) :\leftrightarrow \exists A\ (\top\colon A \times A \to A)$$

— label: `dfn_LawComp`

$$(\top\colon A \times A \to A) \leftrightarrow \begin{cases} \mathsf{LawComp}(\top) \\ \underline{\top} = A \end{cases}$$

Definition 1.4 — $\top$ on A is associative

$$\mathsf{Assoc}(\top; A) :\leftrightarrow \begin{cases} \top\colon A \times A \to A \\ \forall a, b, c \in A\ ((a \top b) \top c = a \top (b \top c)) \end{cases}$$

— label: `dfn_Assoc`

Example: [a] [b]

1. $\mathsf{Assoc}\left(\top_{+_{\mathbb{Z}}}; \mathbb{Z}\right)$
2. $\mathsf{Assoc}\left(\top_{\cdot_{\mathbb{Z}}}; \mathbb{Z}\right)$
3. $\mathsf{Assoc}\left(\top_{\circ, S}; {}^{S}S\right)$
4. $\neg\,\mathsf{Assoc}\left(\top_{-_{\mathbb{Z}}}; \mathbb{Z}\right)$

[a] $\top_{+_\mathbb{Z}} := \{\langle\langle x, y\rangle, x +_\mathbb{Z} y\rangle \mid x, y \in \mathbb{Z}\}$ etc.
[b] $\top_{\circ,S} := \left\{\langle\langle f, g\rangle, g \circ f\rangle \mid f, g \in {}^S S\right\}$

Definition 1.5 — e is a neutral element for $\top$ in A

$$\mathsf{Neut}(e; \top, A) :\leftrightarrow \begin{cases} \top \colon A \times A \to A \\ e \in A \\ \forall a \in A\ (a \top e = e \top a = a) \end{cases}$$

— label: `dfn_Neut`

Example:

1. $$\mathsf{Neut}\big(0_\mathbb{Z}; \top_{+_\mathbb{Z}}, \mathbb{Z}\big)$$
2. $$\mathsf{Neut}\big(1_\mathbb{Z}; \top_{\cdot_\mathbb{Z}}, \mathbb{Z}\big)$$
3. $$\mathsf{Neut}\big(\mathrm{id}_S; \top_{\circ,S}\big)$$
4. $$\forall x \in \mathbb{Z}\ \neg\,\mathsf{Neut}\big(x; \top_{-_\mathbb{Z}}, \mathbb{Z}\big)$$

Theorem 1.6 — Uniqueness of neutral element

$$!e\ \ \mathsf{Neut}(e; \top, A)$$

— label: `thm_neut_unq`

Proof: Assume $\mathsf{Neut}(e_\mathbf{1}; \top, A)$ and $\mathsf{Neut}(e_\mathbf{2}; \top, A)$. Then, by Definition 1.5,

$$e_\mathbf{1}, e_\mathbf{2} \in A$$
$$\forall a \in A\ (e_\mathbf{1} \top a = a)$$
$$\forall a \in A\ (a \top e_\mathbf{2} = a)$$

Thus, $e_\mathbf{1} = e_\mathbf{1} \top e_\mathbf{2} = e_\mathbf{2}$.

Definition 1.7 — Neutral element for $\top$ in A

Define $e_\top$ as e in Theorem 1.6:

$$\exists e\ \ \mathsf{Neut}(e; \top, A) \to \mathsf{Neut}\big(e_{\top,A}; \top, A\big)$$
$$\text{Otherwise} \to e_{\top,A} = \mathbf{U}$$

— label: `dfn_neut`

Convention 1.8

1. Syn. for $e_{+,\underline{\pm}}$ —
$$\mathsf{0}$$
2. Syn. for $e_{\cdot,\underline{\div}}$ —
$$\mathsf{1}$$

Definition 1.9 — A is a monoid for $\top$

$$\mathsf{Monoid}(A; \top) :\leftrightarrow \begin{cases} \mathsf{Assoc}(\top; A) \\ \exists e\ \ \mathsf{Neut}(e; \top, A) \end{cases}$$

— label: `dfn_Monoid`

$$\mathsf{Monoid}(A; \top) \leftrightarrow \begin{cases} \top \colon A \times A \to A \\ \forall a, b, c \in A\ ((a \top b) \top c = a \top (b \top c)) \\ e_{\top,A} \in A \\ \forall a \in A\ (a \top e_{\top,A} = e_{\top,A} \top a = a) \end{cases}$$

$$\mathsf{Monoid}(A; \top) \to \mathsf{Monoid}(\underline{\top}; \top)$$

Proposition 1.10

$$\begin{cases} \mathsf{Monoid}(\underline{\top}; \top) \\ n \in \omega \\ a\colon [1,n] \to \underline{\top} \end{cases} \to \exists! F\colon [0,n] \to \underline{\top} \begin{cases} F(0) = e_{\top,\underline{\top}} \\ \forall m \in [0,n^-]\ F(m^+) = F(m) \top a_{m^+} \end{cases}$$

— label: `thm_compSeq`

Proof: (Prove by Induction)

(1) Assume (A1) $\mathsf{Monoid}(\underline{\top}; \top)$ and (A2) $a\colon [1,0] \to \underline{\top}$.
By $m \notin [0,0^-]$, (P1) $\forall m \in [0,0^-]\ F(m^+) = F(m) \top a_{m^+}$.
Let us prove

$$\exists! F\colon [0,n] \to \underline{\top} \begin{cases} F(0) = e_{\top,\underline{\top}} \\ \forall m \in [0,n^-]\ F(m^+) = F(m) \top a_{m^+} \end{cases}$$

Existence Let $F = \{\langle 0, e_{\top,\underline{\top}}\rangle\}$. Then,
(1.1) By (A1), $e_{\top,\underline{\top}} \in \underline{\top}$. Thus, $F\colon [0,0] \to \underline{\top}$.
(1.2) $F(0) = e_{\top,\underline{\top}}$.
Thus, by (P1),

$$\exists F\colon [0,0] \to \underline{\top} \begin{cases} F(0) = e_{\top,\underline{\top}} \\ \forall m \in [0,0^-]\ F(m^+) = F(m) \top a_{m^+} \end{cases}$$

Uniqueness Assume such F exists.
By $F\colon [0,n] \to \underline{\top}$, $\exists x\ F = \{\langle 0, x\rangle\}$. Take such x.
Thus, $x = F(0) = e_{\top,\underline{\top}}$.
Thus, $F = \{\langle 0, e_{\top,\underline{\top}}\rangle\}$, which is unique.

(2) Assume (A1)

$$\begin{cases} \mathsf{Monoid}(\underline{\top}; \top) \\ a\colon [1,n] \to \underline{\top} \end{cases} \to \exists! F\colon [0,n] \to \underline{\top} \begin{cases} F(0) = e_{\top,\underline{\top}} \\ \forall m \in [0,n^-]\ F(m^+) = F(m) \top a_{m^+} \end{cases}$$

, (A2) $\mathsf{Monoid}(\underline{\top}; \top)$ and (A3) $a\colon [1,n^+] \to \underline{\top}$.
Let $b = a\restriction_{[1,n]}$. Then, $b\colon [1,n] \to \underline{\top}$.
Thus, by (A1, A2),

$$\exists! F\colon [0,n] \to \underline{\top} \begin{cases} F(0) = e_{\top,\underline{\top}} \\ \forall m \in [0,n^-]\ F(m^+) = F(m) \top b_{m^+} \end{cases}$$

Take such unique F.
Let $G = F \cup \{\langle n^+, F(n) \top a_{n^+}\rangle\}$. Then,
(2.1) $G(0) = F(0) = e_{\top,\underline{\top}}$.
(2.2) Assume $m \in [0,n]$.
If $m \in [0,n^-]$,

$$G(m^+) = F(m^+) = F(m) \top a_{m^+} = G(m) \top a_{m^+}$$

If $m = n$,

$$G(m^+) = G(n^+) = F(n) \top a_{n^+} = G(n) \top a_{n^+}$$

Thus,

$$\begin{cases} G\colon [0,n^+] \to \underline{\top} G(0) = e_{\top,\underline{\top}} \\ \forall m \in [0,n]\ G(m^+) = G(m) \top a_{m^+} \end{cases}$$

Since F is unique, G is unique.
Thus,

$$\exists! F\colon [0,n^+] \to \underline{\top} \begin{cases} F(0) = e_{\top,\underline{\top}} \\ \forall m \in [0,n]\ F(m^+) = F(m) \top a_{m^+} \end{cases}$$

Definition 1.11 — Composite of a finite sequence

Define $\mathop{\top}\limits^{n} a$ as $F(n)$ in Proposition 1.10:

$$\begin{cases} \mathsf{Monoid}(\underline{\top};\top) \\ n \in \omega \\ a\colon [1,n] \to \underline{\top} \end{cases} \to \begin{cases} \mathop{\top}\limits_{} a\colon [0,n] \to \underline{\top} \\ \mathop{\top}\limits^{0} a = e_{\top,\underline{\top}} \\ \forall m \in [0,n^-]\ \mathop{\top}\limits^{m^+} a = \left(\mathop{\top}\limits^{m} a\right) \top a_{m^+} \end{cases}$$

$$\text{Otherwise} \to \mathop{\top}\limits_{} a = \mathbf{U}$$

— label: `dfn_compSeq`

Example: Assume $s = \{\langle 1,a\rangle, \langle 2,b\rangle, \langle 3,c\rangle, \langle 4,d\rangle\}$, $a,b,c,d \in A$ and $\mathsf{Monoid}(A;\top)$. Then, $\mathsf{Monoid}(\underline{\top};\top)$ and $s\colon [1,4] \to \underline{\top}$. Thus,

1. $$\mathop{\top}\limits^{1} s = \left(\mathop{\top}\limits^{0} s\right) \top s_1 = e_{\top,\underline{\top}} \top a = a$$
2. $$\mathop{\top}\limits^{3} s = \left(\mathop{\top}\limits^{2} s\right) \top s_3 = \left(\left(\mathop{\top}\limits^{1} s\right) \top s_2\right) \top s_3 = (a \top b) \top c$$
3. $$\mathop{\top}\limits^{4} s = \left(\mathop{\top}\limits^{3} s\right) \top s_4 = ((a \top b) \top c) \top d$$

Convention 1.12

1. Syn. for $\mathop{\top}\limits^{n} a = \mathop{\top}\limits^{n} \{\langle i, a_i\rangle \mid i \in \omega\}$ —
$$\mathop{\top}\limits_{i=1}^{n} a_i \ /\ a_1 \top \cdots \top a_n$$
2. Syn. for $\mathop{+}\limits_{i=1}^{n} a_i$ —
$$\sum_{i=1}^{n} a_i$$
3. Syn. for $\mathop{\bullet}\limits_{i=1}^{n} a_i$ —
$$\prod_{i=1}^{n} a_i$$

Definition 1.13

$$\mathop{\top}\limits_{i=m}^{n} a_i := \mathop{\top}\limits_{i=1}^{n-m+1} \big\{\langle j, a_{j+m-1}\rangle \mid j \in \omega\big\}_i$$