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

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

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

— label: `dfn_uds`

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

Definition 1.3 — $\top$ 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 1.4 — 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 1.5 — 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 1.4,

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

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

Definition 1.6 — Neutral element for $\top$ in A

Define $e_{\top}$ as e in Theorem 1.5:

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

— label: `dfn_neut`

Convention 1.7

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

Definition 1.8 — 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`

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

Proposition 1.9

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

— 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 1.10 — Composite of a finite sequence

Define $\mathop{\top}\limits^{n} a$ as $F(n)$ in Proposition 1.9:

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

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

— label: `dfn_compSeq`

Example: Let $s=\{\langle 1,a\rangle,\langle 2,b\rangle,\langle 3,c\rangle,\langle 4,d\rangle\}$. Assume $a,b,c,d\in A$ 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. $$\mathop{\top}\limits^{4} s=\left(\mathop{\top}\limits^{3} s\right)\top s_4 = ((a\top b)\top c)\top d$$

Definition 1.11

$$\mathop{\top}\limits_{i=m}^{n}\tau := \mathop{\top}\limits^{n-m+1}\{\langle i,\tau[i+m-1/i]\rangle\mid i\in[1,n-m+1]\}$$

— label: `dfn_CompSeqMN`

$$\begin{cases}\mathsf{Monoid}(A;\top)\\ n\in\omega\ a\colon[1,n]\to A\end{cases}\to \mathop{\top}\limits_{i=1}^{n} a_i = \mathop{\top}\limits^{n} a$$

Convention 1.12

1. Syn. for $\mathop{+}\limits_{i=m}^{n} a_i$ —
$$\sum_{i=m}^{n} a_i$$
2. Syn. for $\mathop{\boldsymbol{\cdot}}\limits_{i=m}^{n} a_i$ —
$$\prod_{i=m}^{n} a_i$$

Theorem 1.13 — General associativity theorem

$$\begin{cases}\mathsf{Monoid}(A;\top)\\ n\in\omega,\ \ a\colon[1,n]\to A\\ h\in\omega,\ \ k\colon[1,h^+]\to\omega\\ k_1=1,\ \ k_{h^+}=n^+\\ \forall m\in[1,h]\ (k_m\le k_{m^+})\end{cases}\to \mathop{\top}\limits_{i=1}^{n} a_i = \mathop{\top}\limits_{i=1}^{h}\mathop{\top}\limits_{j=k_i}^{k_{i^+}-1} a_j$$

— label: `thm_genAssoc`

Proof:

Definition 1.14

$$a^{n,\top} := \top_{i=1}^{n} a$$

— label: dfn_pow

Convention 1.15

1. Syn. for $a^{n,+}$ —

$$na$$

2. Syn. for $a^{n,\cdot}$ —

$$a^n$$

Theorem 1.16

$$\begin{cases} \mathsf{Monoid}(A;\top) \\ a \in A \\ 0 \neq m, n \in \omega \end{cases} \rightarrow$$

1. $$a^{0,\top} = e_{\top,A}$$
2. $$a^{1,\top} = a$$
3. $$a^{m+n,\top} = a^{m,\top} \top a^{n,\top}$$
4. $$a^{m\cdot n,\top} = (a^{m,\top})^{n,\top}$$

Proof:

1. $$0a = 0, \quad a^0 = 1$$
2. $$1a = a, \quad a^1 = a$$
3. $$(m+n)a = ma + na, \quad a^{m+n} = a^m a^n$$
4. $$(m \cdot n)a = m(na), \quad a^{m \cdot n} = (a^m)^n$$

Definition 1.17 — A is a [commutative/Abelian] monoid

$$\mathsf{CommMonoid}(A;\top) :\leftrightarrow \begin{cases} \mathsf{Monoid}(A;\top) \\ \forall a, b \in A \ (a \top b = b \top a) \end{cases}$$

— label: dfn_CommMonoid

Example:

1. $$\mathsf{CommMonoid}\big(\mathbb{Z}; \top_{+_{\mathbb{Z}}}\big)$$
2. $$\mathsf{CommMonoid}\big(\mathbb{Z}; \top_{\cdot_{\mathbb{Z}}}\big)$$
3. $$\neg\,\mathsf{CommMonoid}\big({}^{\mathbb{R}}\mathbb{R}; \top_{\circ,\mathbb{R}}\big)$$

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

Theorem 1.18 — General commutativity theorem

$$\begin{cases} \mathsf{CommMonoid}(A;\top) \\ n \in \omega, \ a \colon [1,n] \to A \\ \varpi \colon [1,n] \rightleftarrows [1,n] \end{cases} \rightarrow \top_{i=1}^{n} a_i = \top_{i=1}^{n} a_{\varpi(i)}$$

— label: thm_genComm