WARSAW UNIVERSITY

ALEGEBRAIC STRUCTURES

Piotr M. Hajac

January 2013

One binary associative composition law

Let G be a non-empty set. The map $G \times G \ni (a, b) \mapsto ab \in G$ is called an associative composition law if and only if

$$\boxed{\forall\, a, b, c \in G \colon a(bc) = (ab)c}\,.$$

One binary associative composition law

Let G be a non-empty set. The map $G \times G \ni (a, b) \mapsto ab \in G$ is called an associative composition law if and only if

$$\boxed{\forall\, a, b, c \in G \colon a(bc) = (ab)c}\,.$$

Algebraic structures with such a composition law are listed below from the most to the least general. Each step adds an assumption, so that each of these structures is a special case of the preceding structures.

One binary associative composition law

Let G be a non-empty set. The map $G \times G \ni (a, b) \mapsto ab \in G$ is called an associative composition law if and only if

$$\boxed{\forall\, a, b, c \in G \colon a(bc) = (ab)c}\,.$$

Algebraic structures with such a composition law are listed below from the most to the least general. Each step adds an assumption, so that each of these structures is a special case of the preceding structures.

1. Semigroups: no assumptions. Example: the set of all finite words written with two letters (ab, ba, $abba$,...).

One binary associative composition law

Let G be a non-empty set. The map $G \times G \ni (a, b) \mapsto ab \in G$ is called an associative composition law if and only if

$$\boxed{\forall\, a, b, c \in G \colon a(bc) = (ab)c}\,.$$

Algebraic structures with such a composition law are listed below from the most to the least general. Each step adds an assumption, so that each of these structures is a special case of the preceding structures.

1. Semigroups: no assumptions. Example: the set of all finite words written with two letters (ab, ba, $abba$,...).
2. Monoids: $\exists\, e \in G\, \forall\, g \in G \colon eg = g = ge$.
   Examples: $(\mathrm{Map}(X, X), \circ, \mathrm{id})$, $(\mathbb{N}, +, 0)$.

One binary associative composition law

Let G be a non-empty set. The map $G \times G \ni (a, b) \mapsto ab \in G$ is called an associative composition law if and only if

$$\boxed{\forall\, a, b, c \in G\colon a(bc) = (ab)c}\,.$$

Algebraic structures with such a composition law are listed below from the most to the least general. Each step adds an assumption, so that each of these structures is a special case of the preceding structures.

1. Semigroups: no assumptions. Example: the set of all finite words written with two letters (ab, ba, $abba$,...).
2. Monoids: $\exists\, e \in G\, \forall\, g \in G\colon eg = g = ge$.
   Examples: $(\mathrm{Map}(X, X), \circ, \mathrm{id})$, $(\mathbb{N}, +, 0)$.
3. Groups: $\forall\, g \in G\, \exists\, g^{-1} \in G\colon g^{-1}g = e = gg^{-1}$.
   Examples: $(\mathrm{Bij}(X, X), \circ, \mathrm{id})$, $(S_n, \circ, \mathrm{id})$.

One binary associative composition law

Let G be a non-empty set. The map $G \times G \ni (a, b) \mapsto ab \in G$ is called an associative composition law if and only if

$$\boxed{\forall\, a, b, c \in G\colon a(bc) = (ab)c}\,.$$

Algebraic structures with such a composition law are listed below from the most to the least general. Each step adds an assumption, so that each of these structures is a special case of the preceding structures.

1. Semigroups: no assumptions. Example: the set of all finite words written with two letters (ab, ba, $abba$,...).
2. Monoids: $\exists\, e \in G\, \forall\, g \in G\colon eg = g = ge$.
   Examples: $(\mathrm{Map}(X, X), \circ, \mathrm{id})$, $(\mathbb{N}, +, 0)$.
3. Groups: $\forall\, g \in G\, \exists\, g^{-1} \in G\colon g^{-1}g = e = gg^{-1}$.
   Examples: $(\mathrm{Bij}(X, X), \circ, \mathrm{id})$, $(S_n, \circ, \mathrm{id})$.
4. Abelian groups: $\forall\, g, h \in G\colon gh = hg$.
   Examples: $(\mathbb{Z}, +, 0)$, $(\mathbb{Z}/n\mathbb{Z}, +, 0)$.

Two distributive composition laws

Let R be a non-empty set with two binary associative composition laws satisfying the distributivity condition:

$$\boxed{\forall\, r, s, t \in R\colon (r+s)t = rt + st,\ r(s+t) = rs + rt}\ .$$

Two distributive composition laws

Let R be a non-empty set with two binary associative composition laws satisfying the distributivity condition:

$$\boxed{\forall\, r, s, t \in R\colon (r+s)t = rt + st,\ r(s+t) = rs + rt}\,.$$

Algebraic structures with two such composition laws are listed below the same way as before.

Two distributive composition laws

Let R be a non-empty set with two binary associative composition laws satisfying the distributivity condition:

$$\boxed{\forall\, r,s,t \in R\colon (r+s)t = rt + st,\ r(s+t) = rs + rt}\,.$$

Algebraic structures with two such composition laws are listed below the same way as before.

1. Rings: $(R,+,0)$ is an Abelian group and $(R,\cdot,1)$ is a monoid. Examples: $(\mathrm{End}_{\mathbb{Z}}(G);\circ,\mathrm{id};$ poinwise $+,0$ function$)$, where $(G,+,0)$ is an Abelian group, matrix ring $M_n(\mathbb{Z})$.

Two distributive composition laws

Let R be a non-empty set with two binary associative composition laws satisfying the distributivity condition:

$$\boxed{\forall\, r,s,t \in R\colon (r+s)t = rt + st,\ r(s+t) = rs + rt}\,.$$

Algebraic structures with two such composition laws are listed below the same way as before.

1. Rings: $(R,+,0)$ is an Abelian group and $(R,\cdot,1)$ is a monoid.
   Examples: $(\mathrm{End}_{\mathbb{Z}}(G);\circ,\mathrm{id};$ poinwise $+,0$ function$)$, where $(G,+,0)$ is an Abelian group, matrix ring $M_n(\mathbb{Z})$.
2. Commutative rings: $\forall\, r,s \in R\colon rs = sr$.
   Examples: $(\mathbb{Z}/n\mathbb{Z};\cdot,1;+,0)$, polynomial ring $(\mathbb{Z}/n\mathbb{Z})[\mathbb{N}]$.

Two distributive composition laws

Let R be a non-empty set with two binary associative composition laws satisfying the distributivity condition:

$$\boxed{\forall\, r,s,t \in R\colon (r+s)t = rt + st,\ r(s+t) = rs + rt}\,.$$

Algebraic structures with two such composition laws are listed below the same way as before.

1. Rings: $(R,+,0)$ is an Abelian group and $(R,\cdot,1)$ is a monoid.
   Examples: $(\mathrm{End}_{\mathbb{Z}}(G);\circ,\mathrm{id};$ poinwise $+,0$ function$)$, where $(G,+,0)$ is an Abelian group, matrix ring $M_n(\mathbb{Z})$.
2. Commutative rings: $\forall\, r,s \in R\colon rs = sr$.
   Examples: $(\mathbb{Z}/n\mathbb{Z};\cdot,1;+,0)$, polynomial ring $(\mathbb{Z}/n\mathbb{Z})[\mathbb{N}]$.
3. Integral domains: $rs = 0 \Rightarrow (r = 0$ or $s = 0)$.
   Examples: $(\mathbb{Z};\cdot,1;+,0)$, polynomial ring $\mathbb{Z}[\mathbb{N}]$.

Two distributive composition laws

Let R be a non-empty set with two binary associative composition laws satisfying the distributivity condition:

$$\boxed{\forall\, r,s,t \in R\colon (r+s)t = rt + st,\ r(s+t) = rs + rt}\,.$$

Algebraic structures with two such composition laws are listed below the same way as before.

1. Rings: $(R,+,0)$ is an Abelian group and $(R,\cdot,1)$ is a monoid.
   Examples: $(\mathrm{End}_{\mathbb{Z}}(G);\circ,\mathrm{id};$ poinwise $+,0$ function$)$, where $(G,+,0)$ is an Abelian group, matrix ring $M_n(\mathbb{Z})$.
2. Commutative rings: $\forall\, r,s \in R\colon rs = sr$.
   Examples: $(\mathbb{Z}/n\mathbb{Z};\cdot,1;+,0)$, polynomial ring $(\mathbb{Z}/n\mathbb{Z})[\mathbb{N}]$.
3. Integral domains: $rs = 0 \Rightarrow (r = 0$ or $s = 0)$.
   Examples: $(\mathbb{Z};\cdot,1;+,0)$, polynomial ring $\mathbb{Z}[\mathbb{N}]$.
4. Fields: $(R\setminus\{0\},\cdot,1)$ is a group.
   Examples: $(\mathbb{Z}/p\mathbb{Z};\cdot,1;+,0)$, where p is a prime number.

Two distributive composition laws

Let R be a non-empty set with two binary associative composition laws satisfying the distributivity condition:

$$\boxed{\forall\, r, s, t \in R\colon (r+s)t = rt + st,\ r(s+t) = rs + rt}\,.$$

Algebraic structures with two such composition laws are listed below the same way as before.

1. Rings: $(R, +, 0)$ is an Abelian group and $(R, \cdot, 1)$ is a monoid.
   Examples: $(\mathrm{End}_{\mathbb{Z}}(G); \circ, \mathrm{id};$ poinwise $+, 0$ function$)$, where $(G, +, 0)$ is an Abelian group, matrix ring $M_n(\mathbb{Z})$.
2. Commutative rings: $\forall\, r, s \in R\colon rs = sr$.
   Examples: $(\mathbb{Z}/n\mathbb{Z}; \cdot, 1; +, 0)$, polynomial ring $(\mathbb{Z}/n\mathbb{Z})[\mathbb{N}]$.
3. Integral domains: $rs = 0 \Rightarrow (r = 0$ or $s = 0)$.
   Examples: $(\mathbb{Z}; \cdot, 1; +, 0)$, polynomial ring $\mathbb{Z}[\mathbb{N}]$.
4. Fields: $(R \setminus \{0\}, \cdot, 1)$ is a group.
   Examples: $(\mathbb{Z}/p\mathbb{Z}; \cdot, 1; +, 0)$, where p is a prime number.
5. Fields of characteristic 0: contain $\mathbb{Q}$ as a subfield.
   Examples: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Distributive actions on Abelian groups

Let M be an Abelian group and R a ring equipped with an associative composition law:

$$\boxed{R \times M \ni (r, m) \longmapsto rm \in M} \, .$$

Distributive actions on Abelian groups

Let M be an Abelian group and R a ring equipped with an associative composition law:

$$\boxed{R \times M \ni (r, m) \longmapsto rm \in M} \, .$$

Such algebraic structures are listed below the same way as before.

Distributive actions on Abelian groups

Let M be an Abelian group and R a ring equipped with an associative composition law:

$$\boxed{R \times M \ni (r, m) \longmapsto rm \in M}\,.$$

Such algebraic structures are listed below the same way as before.

1. Modules: $\forall\, m, n \in M, r, s \in R$:
   $(r+s)m = rm + sm,\ r(m+n) = rm + rn,\ 1m = m.$
   Examples: $\mathrm{End}_{\mathbb{Z}}(G) \times G \ni (f, g) \mapsto f(g) \in G$
   and $\mathbb{Z}^n$ over the matrix ring $M_n(\mathbb{Z})$.

Distributive actions on Abelian groups

Let M be an Abelian group and R a ring equipped with an associative composition law:

$$\boxed{R \times M \ni (r, m) \longmapsto rm \in M}\,.$$

Such algebraic structures are listed below the same way as before.

1. Modules: $\forall\, m, n \in M, r, s \in R$:
   $(r+s)m = rm + sm,\ r(m+n) = rm + rn,\ 1m = m.$
   Examples: $\mathrm{End}_{\mathbb{Z}}(G) \times G \ni (f, g) \mapsto f(g) \in G$
   and $\mathbb{Z}^n$ over the matrix ring $M_n(\mathbb{Z})$.
2. Free modules: there exists a basis of M. Example: $\bigoplus_{\mathbb{N}} R$.

Distributive actions on Abelian groups

Let M be an Abelian group and R a ring equipped with an associative composition law:

$$\boxed{R \times M \ni (r, m) \longmapsto rm \in M}\,.$$

Such algebraic structures are listed below the same way as before.

1. Modules: $\forall\, m, n \in M, r, s \in R$:
   $(r+s)m = rm + sm,\ r(m+n) = rm + rn,\ 1m = m.$
   Examples: $\mathrm{End}_{\mathbb{Z}}(G) \times G \ni (f, g) \mapsto f(g) \in G$
   and $\mathbb{Z}^n$ over the matrix ring $M_n(\mathbb{Z})$.
2. Free modules: there exists a basis of M. Example: $\bigoplus_{\mathbb{N}} R$.
3. Vector spaces: R is a field. Example: $\bigoplus_{\mathbb{N}} R$.

Distributive actions on Abelian groups

Let M be an Abelian group and R a ring equipped with an associative composition law:

$$\boxed{R \times M \ni (r, m) \longmapsto rm \in M}\,.$$

Such algebraic structures are listed below the same way as before.

1. Modules: $\forall\, m, n \in M, r, s \in R$:
   $(r+s)m = rm + sm,\ r(m+n) = rm + rn,\ 1m = m.$
   Examples: $\mathrm{End}_{\mathbb{Z}}(G) \times G \ni (f, g) \mapsto f(g) \in G$
   and $\mathbb{Z}^n$ over the matrix ring $M_n(\mathbb{Z})$.
2. Free modules: there exists a basis of M. Example: $\bigoplus_{\mathbb{N}} R$.
3. Vector spaces: R is a field. Example: $\bigoplus_{\mathbb{N}} R$.
4. Finite-dimensional vector spaces: there exists a finite basis of M. Example: R^n.

Algebras over commutative rings

Let A be a module over a commutative ring k equipped with a k-bilinear associative multiplication

$$\boxed{A \times A \ni (a, b) \longmapsto ab \in A}\,.$$

Then A is called an algebra over k.

Algebras over commutative rings

Let A be a module over a commutative ring k equipped with a k-bilinear associative multiplication

$$\boxed{A \times A \ni (a, b) \longmapsto ab \in A}\,.$$

Then A is called an algebra over k.

It is called a unital algebra over k if and only if A is a ring with respect to its Abelian group structure and multiplication. In other words, a unital algebra is a module with a linear ring structure, or a ring with a compatible module structure. Every ring is a unital algebra over the ring $\mathbb{Z}$ of all integers.

Spectrum, eigenvectors and eigenvalues

Let A be a unital algebra over a commutative ring k. The spectrum of $a \in A$ is the following subset of k:

$$\boxed{\mathrm{spec}_A(a) := \{\lambda \in k \mid \nexists\, (a - \lambda 1)^{-1} \in A\}}\,.$$

Spectrum, eigenvectors and eigenvalues

Let A be a unital algebra over a commutative ring k. The spectrum of $a \in A$ is the following subset of k:

$$\boxed{\mathrm{spec}_A(a) := \{\lambda \in k \mid \nexists\, (a - \lambda 1)^{-1} \in A\}}\,.$$

In particular, when M is a module over k, we can take $A = \mathrm{End}_k(M)$. Then $v \in M$ is called an eigenvector of $a \in \mathrm{End}_k(M)$ corresponding to $\lambda \in k$ if and only if

$$av = \lambda v.$$

Note that $v \neq 0 \;\Rightarrow\; \lambda \in \mathrm{spec}_A(a)$. All elements of $\mathrm{spec}_A(a)$ coming from a non-zero eigenvector of a are called eigenvalues.

Spectrum, eigenvectors and eigenvalues

Let A be a unital algebra over a commutative ring k. The spectrum of $a \in A$ is the following subset of k:

$$\boxed{\mathrm{spec}_A(a) := \{\lambda \in k \mid \nexists\, (a - \lambda 1)^{-1} \in A\}}\,.$$

In particular, when M is a module over k, we can take $A = \mathrm{End}_k(M)$. Then $v \in M$ is called an eigenvector of $a \in \mathrm{End}_k(M)$ corresponding to $\lambda \in k$ if and only if

$$av = \lambda v.$$

Note that $v \neq 0 \;\Rightarrow\; \lambda \in \mathrm{spec}_A(a)$. All elements of $\mathrm{spec}_A(a)$ coming from a non-zero eigenvector of a are called eigenvalues.

If M is a finite-dimensional free module over a non-zero commutative ring k, then all elements of the spectrum of any endomorphism a are eigenvalues. They are roots of the characteristic polynomial

$$\boxed{\det(a - \lambda\,\mathrm{id})}\,.$$