

Free Algebras, especially groups

Modern Algebra 1

Fall 2016

Let \mathcal{C} be a category of algebras in the same language, defined by some set Σ of identities, and taking for morphisms all homomorphisms between algebras in \mathcal{C} .

Let \mathcal{C} be a category of algebras in the same language, defined by some set Σ of identities, and taking for morphisms all homomorphisms between algebras in \mathcal{C} . (E.g. \mathcal{C} could be the category of all groups, all abelian groups, all rings, Boolean algebras, \mathbb{F} -vector spaces,)

Let \mathcal{C} be a category of algebras in the same language, defined by some set Σ of identities, and taking for morphisms all homomorphisms between algebras in \mathcal{C} . (E.g. \mathcal{C} could be the category of all groups, all abelian groups, all rings, Boolean algebras, \mathbb{F} -vector spaces,)

Free algebras of all ranks exist in \mathcal{C} , and they can be constructed from sets of words.

Let \mathcal{C} be a category of algebras in the same language, defined by some set Σ of identities, and taking for morphisms all homomorphisms between algebras in \mathcal{C} . (E.g. \mathcal{C} could be the category of all groups, all abelian groups, all rings, Boolean algebras, \mathbb{F} -vector spaces,)

Free algebras of all ranks exist in \mathcal{C} , and they can be constructed from sets of words.

To illustrate, suppose \mathcal{C} is the category of all algebras with one binary operation subject to the identities in Σ where $\Sigma = \{\forall x \forall y (x \cdot y = y \cdot x)\}$.

Let \mathcal{C} be a category of algebras in the same language, defined by some set Σ of identities, and taking for morphisms all homomorphisms between algebras in \mathcal{C} . (E.g. \mathcal{C} could be the category of all groups, all abelian groups, all rings, Boolean algebras, \mathbb{F} -vector spaces,)

Free algebras of all ranks exist in \mathcal{C} , and they can be constructed from sets of words.

To illustrate, suppose \mathcal{C} is the category of all algebras with one binary operation subject to the identities in Σ where $\Sigma = \{\forall x \forall y (x \cdot y = y \cdot x)\}$.

Construction of a free \mathcal{C} -algebra over X :

- 1 Create the set $W(X)$ of all \mathcal{C} -words (= “formal expressions”) over X .

Let \mathcal{C} be a category of algebras in the same language, defined by some set Σ of identities, and taking for morphisms all homomorphisms between algebras in \mathcal{C} . (E.g. \mathcal{C} could be the category of all groups, all abelian groups, all rings, Boolean algebras, \mathbb{F} -vector spaces,)

Free algebras of all ranks exist in \mathcal{C} , and they can be constructed from sets of words.

To illustrate, suppose \mathcal{C} is the category of all algebras with one binary operation subject to the identities in Σ where $\Sigma = \{\forall x \forall y (x \cdot y = y \cdot x)\}$.

Construction of a free \mathcal{C} -algebra over X :

- 1 Create the set $W(X)$ of all \mathcal{C} -words (= “formal expressions”) over X .
- 2 Factor by \mathcal{C} -equivalence.

Example in more detail

Example in more detail

Suppose that $X = \{x_1, x_2, \dots\}$.

Example in more detail

Suppose that $X = \{x_1, x_2, \dots\}$.

$$W(X) = \{x_1, x_2, \dots, (x_1 \cdot x_1), (x_1 \cdot x_2), \dots, (x_1 \cdot (x_2 \cdot x_3)), ((x_2 \cdot x_3) \cdot x_1), \dots\}.$$

Example in more detail

Suppose that $X = \{x_1, x_2, \dots\}$.

$$W(X) = \{x_1, x_2, \dots, (x_1 \cdot x_1), (x_1 \cdot x_2), \dots, (x_1 \cdot (x_2 \cdot x_3)), ((x_2 \cdot x_3) \cdot x_1), \dots\}.$$

Note that $(x_1 \cdot (x_2 \cdot x_3)) \equiv_{\mathcal{C}} (x_1 \cdot (x_3 \cdot x_2)) \equiv_{\mathcal{C}} ((x_2 \cdot x_3) \cdot x_1) \equiv_{\mathcal{C}} ((x_3 \cdot x_2) \cdot x_1)$.

Example in more detail

Suppose that $X = \{x_1, x_2, \dots\}$.

$W(X) = \{x_1, x_2, \dots, (x_1 \cdot x_1), (x_1 \cdot x_2), \dots, (x_1 \cdot (x_2 \cdot x_3)), ((x_2 \cdot x_3) \cdot x_1), \dots\}$.

Note that $(x_1 \cdot (x_2 \cdot x_3)) \equiv_{\mathcal{C}} (x_1 \cdot (x_3 \cdot x_2)) \equiv_{\mathcal{C}} ((x_2 \cdot x_3) \cdot x_1) \equiv_{\mathcal{C}} ((x_3 \cdot x_2) \cdot x_1)$.

We may take $\mathbb{F}_{\mathcal{C}}(X) = W(X)/\equiv$, or we may build $\mathbb{F}_{\mathcal{C}}(X)$ out of a set consisting of one representative word from each \mathcal{C} -equivalence class of words (a normal form).

Example in more detail

Suppose that $X = \{x_1, x_2, \dots\}$.

$W(X) = \{x_1, x_2, \dots, (x_1 \cdot x_1), (x_1 \cdot x_2), \dots, (x_1 \cdot (x_2 \cdot x_3)), ((x_2 \cdot x_3) \cdot x_1), \dots\}$.

Note that $(x_1 \cdot (x_2 \cdot x_3)) \equiv_{\mathcal{C}} (x_1 \cdot (x_3 \cdot x_2)) \equiv_{\mathcal{C}} ((x_2 \cdot x_3) \cdot x_1) \equiv_{\mathcal{C}} ((x_3 \cdot x_2) \cdot x_1)$.

We may take $\mathbb{F}_{\mathcal{C}}(X) = W(X)/\equiv$, or we may build $\mathbb{F}_{\mathcal{C}}(X)$ out of a set consisting of one representative word from each \mathcal{C} -equivalence class of words (a normal form).

The universal property is established like this: given a set-function $X \rightarrow A: x_i \mapsto a_i$, extend it to an algebra homomorphism

$\mathbb{F}_{\mathcal{C}}(X) \rightarrow \mathbb{A}: w(x_1, \dots, x_n) \mapsto w(a_1, \dots, a_n)$ (evaluate the word $w(\bar{x})$ at \bar{a}).

Groups specifically

For groups it is standard to build in some of the equivalence of words into the construction of the words, so we ignore parentheses right away and build in things like $(x^{-1})^{-1} = x$ as well.

Groups specifically

For groups it is standard to build in some of the equivalence of words into the construction of the words, so we ignore parentheses right away and build in things like $(x^{-1})^{-1} = x$ as well.

The construction goes like this:

Groups specifically

For groups it is standard to build in some of the equivalence of words into the construction of the words, so we ignore parentheses right away and build in things like $(x^{-1})^{-1} = x$ as well.

The construction goes like this: This time $W(X)$ is the set of finite, possibly empty strings in the alphabet $X \cup X^{-1}$.

Groups specifically

For groups it is standard to build in some of the equivalence of words into the construction of the words, so we ignore parentheses right away and build in things like $(x^{-1})^{-1} = x$ as well.

The construction goes like this: This time $W(X)$ is the set of finite, possibly empty strings in the alphabet $X \cup X^{-1}$. Define a word to be *reduced* if it has no letter x adjacent to x^{-1} . Group operations are . . .

Groups specifically

For groups it is standard to build in some of the equivalence of words into the construction of the words, so we ignore parentheses right away and build in things like $(x^{-1})^{-1} = x$ as well.

The construction goes like this: This time $W(X)$ is the set of finite, possibly empty strings in the alphabet $X \cup X^{-1}$. Define a word to be *reduced* if it has no letter x adjacent to x^{-1} . Group operations are . . .

When $X = \{x\}$, the set of reduced words is $\{\dots, x^{-1}, e, x, xx, \dots\}$, and $\mathbb{F}_C(x)$ is infinite cyclic.

Groups specifically

For groups it is standard to build in some of the equivalence of words into the construction of the words, so we ignore parentheses right away and build in things like $(x^{-1})^{-1} = x$ as well.

The construction goes like this: This time $W(X)$ is the set of finite, possibly empty strings in the alphabet $X \cup X^{-1}$. Define a word to be *reduced* if it has no letter x adjacent to x^{-1} . Group operations are . . .

When $X = \{x\}$, the set of reduced words is $\{\dots, x^{-1}, e, x, xx, \dots\}$, and $\mathbb{F}_C(x)$ is infinite cyclic. (This is slightly different from the general approach, which would create words like $x, xx, x(xx), (xx)x, \dots$, then define $x(xx) \equiv (xx)x$, etc.)

Outline of the “bare hands” associativity check

Outline of the “bare hands” associativity check

First show that if $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ holds whenever α, β are arbitrary and $|\gamma| = 1$, then it holds for arbitrary α, β, γ .

Outline of the “bare hands” associativity check

First show that if $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ holds whenever α, β are arbitrary and $|\gamma| = 1$, then it holds for arbitrary α, β, γ . Induction on $|\gamma|$:

Outline of the “bare hands” associativity check

First show that if $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ holds whenever α, β are arbitrary and $|\gamma| = 1$, then it holds for arbitrary α, β, γ . Induction on $|\gamma|$:

$$(\alpha\beta)(\gamma x) = ((\alpha\beta)\gamma)x = ((\alpha(\beta\gamma))x) = (\alpha((\beta\gamma)x)) = (\alpha(\beta(\gamma x))).$$

Outline of the “bare hands” associativity check

First show that if $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ holds whenever α, β are arbitrary and $|\gamma| = 1$, then it holds for arbitrary α, β, γ . Induction on $|\gamma|$:

$$(\alpha\beta)(\gamma x) = ((\alpha\beta)\gamma)x = ((\alpha(\beta\gamma))x) = (\alpha((\beta\gamma)x)) = (\alpha(\beta(\gamma x))).$$

Now let $\alpha = \alpha_1 \cdots \alpha_k, k \geq 1, \beta = \beta_1 \cdots \beta_\ell, \ell \geq 1, |\gamma| = 1$, and use induction on $|\beta|$. Write $\alpha \top \beta$ to mean $\alpha_k = \beta_1^{-1}$, $\alpha \perp \beta$ to mean $\alpha_k \neq \beta_1^{-1}$, α_* to mean α minus last letter, $_*\beta$ to mean β minus first letter, etc.

Outline of the “bare hands” associativity check

First show that if $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ holds whenever α, β are arbitrary and $|\gamma| = 1$, then it holds for arbitrary α, β, γ . Induction on $|\gamma|$:

$$(\alpha\beta)(\gamma x) = ((\alpha\beta)\gamma)x = ((\alpha(\beta\gamma))x) = (\alpha((\beta\gamma)x)) = (\alpha(\beta(\gamma x))).$$

Now let $\alpha = \alpha_1 \cdots \alpha_k, k \geq 1, \beta = \beta_1 \cdots \beta_\ell, \ell \geq 1, |\gamma| = 1$, and use induction on $|\beta|$. Write $\alpha \top \beta$ to mean $\alpha_k = \beta_1^{-1}$, $\alpha \perp \beta$ to mean $\alpha_k \neq \beta_1^{-1}$, α_* to mean α minus last letter, $_*\beta$ to mean β minus first letter, etc.

Cases.

❶ $|\beta| = 1, \alpha \top \beta \top \gamma: (\alpha\beta)\gamma = \alpha_*\gamma = \alpha = \alpha e = \alpha(\beta\gamma).$

Outline of the “bare hands” associativity check

First show that if $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ holds whenever α, β are arbitrary and $|\gamma| = 1$, then it holds for arbitrary α, β, γ . Induction on $|\gamma|$:

$$(\alpha\beta)(\gamma x) = ((\alpha\beta)\gamma)x = ((\alpha(\beta\gamma))x) = (\alpha((\beta\gamma)x)) = (\alpha(\beta(\gamma x))).$$

Now let $\alpha = \alpha_1 \cdots \alpha_k, k \geq 1, \beta = \beta_1 \cdots \beta_\ell, \ell \geq 1, |\gamma| = 1$, and use induction on $|\beta|$. Write $\alpha \top \beta$ to mean $\alpha_k = \beta_1^{-1}$, $\alpha \perp \beta$ to mean $\alpha_k \neq \beta_1^{-1}$, α_* to mean α minus last letter, $_*\beta$ to mean β minus first letter, etc.

Cases.

① $|\beta| = 1, \alpha \top \beta \top \gamma: (\alpha\beta)\gamma = \alpha_*\gamma = \alpha = \alpha e = \alpha(\beta\gamma).$

② $|\beta| > 1, \alpha \top \beta \top \gamma:$
 $(\alpha\beta)\gamma = (\alpha_{**}\beta)\gamma = \alpha_*(\beta\gamma) = \alpha_{**}\beta_* = \alpha\beta_* = \alpha(\beta\gamma).$

Outline of the “bare hands” associativity check

First show that if $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ holds whenever α, β are arbitrary and $|\gamma| = 1$, then it holds for arbitrary α, β, γ . Induction on $|\gamma|$:

$$(\alpha\beta)(\gamma x) = ((\alpha\beta)\gamma)x = ((\alpha(\beta\gamma))x) = (\alpha((\beta\gamma)x)) = (\alpha(\beta(\gamma x))).$$

Now let $\alpha = \alpha_1 \cdots \alpha_k, k \geq 1, \beta = \beta_1 \cdots \beta_\ell, \ell \geq 1, |\gamma| = 1$, and use induction on $|\beta|$. Write $\alpha \top \beta$ to mean $\alpha_k = \beta_1^{-1}$, $\alpha \perp \beta$ to mean $\alpha_k \neq \beta_1^{-1}$, α_* to mean α minus last letter, $*\beta$ to mean β minus first letter, etc.

Cases.

- ① $|\beta| = 1, \alpha \top \beta \top \gamma$: $(\alpha\beta)\gamma = \alpha_*\gamma = \alpha = \alpha e = \alpha(\beta\gamma)$.
- ② $|\beta| > 1, \alpha \top \beta \top \gamma$:
 $(\alpha\beta)\gamma = (\alpha_{**}\beta)\gamma = \alpha_*(\beta\gamma) = \alpha_{**}\beta_* = \alpha\beta_* = \alpha(\beta\gamma)$.
- ③ $\alpha \top \beta \perp \gamma$: $(\alpha\beta)\gamma = (\alpha_{**}\beta)\gamma = \alpha_*(\beta\gamma) = \alpha(\beta\gamma)$.

Outline of the “bare hands” associativity check

First show that if $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ holds whenever α, β are arbitrary and $|\gamma| = 1$, then it holds for arbitrary α, β, γ . Induction on $|\gamma|$:

$$(\alpha\beta)(\gamma x) = ((\alpha\beta)\gamma)x = ((\alpha(\beta\gamma))x) = (\alpha((\beta\gamma)x)) = (\alpha(\beta(\gamma x))).$$

Now let $\alpha = \alpha_1 \cdots \alpha_k, k \geq 1, \beta = \beta_1 \cdots \beta_\ell, \ell \geq 1, |\gamma| = 1$, and use induction on $|\beta|$. Write $\alpha \top \beta$ to mean $\alpha_k = \beta_1^{-1}$, $\alpha \perp \beta$ to mean $\alpha_k \neq \beta_1^{-1}$, α_* to mean α minus last letter, $_*\beta$ to mean β minus first letter, etc.

Cases.

- ① $|\beta| = 1, \alpha \top \beta \top \gamma$: $(\alpha\beta)\gamma = \alpha_*\gamma = \alpha = \alpha e = \alpha(\beta\gamma)$.
- ② $|\beta| > 1, \alpha \top \beta \top \gamma$:
 $(\alpha\beta)\gamma = (\alpha_{**}\beta)\gamma = \alpha_*(_*\beta\gamma) = \alpha_{**}\beta_* = \alpha\beta_* = \alpha(\beta\gamma)$.
- ③ $\alpha \top \beta \perp \gamma$: $(\alpha\beta)\gamma = (\alpha_{**}\beta)\gamma = \alpha_*(_*\beta\gamma) = \alpha(\beta\gamma)$.
- ④ $\alpha \perp \beta \top \gamma$: $(\alpha\beta)\gamma = \alpha\beta_* = \alpha(\beta\gamma)$.

Outline of the “bare hands” associativity check

First show that if $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ holds whenever α, β are arbitrary and $|\gamma| = 1$, then it holds for arbitrary α, β, γ . Induction on $|\gamma|$:

$$(\alpha\beta)(\gamma x) = ((\alpha\beta)\gamma)x = ((\alpha(\beta\gamma))x) = (\alpha((\beta\gamma)x)) = (\alpha(\beta(\gamma x))).$$

Now let $\alpha = \alpha_1 \cdots \alpha_k, k \geq 1, \beta = \beta_1 \cdots \beta_\ell, \ell \geq 1, |\gamma| = 1$, and use induction on $|\beta|$. Write $\alpha \top \beta$ to mean $\alpha_k = \beta_1^{-1}$, $\alpha \perp \beta$ to mean $\alpha_k \neq \beta_1^{-1}$, α_* to mean α minus last letter, $_*\beta$ to mean β minus first letter, etc.

Cases.

- ① $|\beta| = 1, \alpha \top \beta \top \gamma$: $(\alpha\beta)\gamma = \alpha_*\gamma = \alpha = \alpha e = \alpha(\beta\gamma)$.
- ② $|\beta| > 1, \alpha \top \beta \top \gamma$:
 $(\alpha\beta)\gamma = (\alpha_{**}\beta)\gamma = \alpha_*(_*\beta\gamma) = \alpha_{**}\beta_* = \alpha\beta_* = \alpha(\beta\gamma)$.
- ③ $\alpha \top \beta \perp \gamma$: $(\alpha\beta)\gamma = (\alpha_{**}\beta)\gamma = \alpha_*(_*\beta\gamma) = \alpha(\beta\gamma)$.
- ④ $\alpha \perp \beta \top \gamma$: $(\alpha\beta)\gamma = \alpha\beta_* = \alpha(\beta\gamma)$.
- ⑤ $\alpha \perp \beta \perp \gamma$: no reduction takes place.

Schreier's Theorem: Subgroups of free groups are free.

Schreier's Theorem: Subgroups of free groups are free.

Q: How do you recognize if a group $F \in \mathcal{C}$ is free in \mathcal{C} over a subset $G \subseteq F$?

Schreier's Theorem: Subgroups of free groups are free.

Q: How do you recognize if a group $F \in \mathcal{C}$ is free in \mathcal{C} over a subset $G \subseteq F$?

A: Show that G is an independent generating set.

Schreier's Theorem: Subgroups of free groups are free.

Q: How do you recognize if a group $F \in \mathcal{C}$ is free in \mathcal{C} over a subset $G \subseteq F$?

A: Show that G is an independent generating set.

G is a *generating set* for F if $F = \langle G \rangle$.

Schreier's Theorem: Subgroups of free groups are free.

Q: How do you recognize if a group $F \in \mathcal{C}$ is free in \mathcal{C} over a subset $G \subseteq F$?

A: Show that G is an independent generating set.

G is a *generating set* for F if $F = \langle G \rangle$.

G is *independent* in F relative to the class \mathcal{C} if every relation $w(\bar{g}) = w'(\bar{g})$ that holds for a tuple of distinct elements in G holds universally in \mathcal{C} .

Schreier's Theorem: Subgroups of free groups are free.

Q: How do you recognize if a group $F \in \mathcal{C}$ is free in \mathcal{C} over a subset $G \subseteq F$?

A: Show that G is an independent generating set.

G is a *generating set* for F if $F = \langle G \rangle$.

G is *independent* in F relative to the class \mathcal{C} if every relation $w(\bar{g}) = w'(\bar{g})$ that holds for a tuple of distinct elements in G holds universally in \mathcal{C} . (Every tuple in every member of \mathcal{C} satisfies the relation.)

Schreier's Theorem: Subgroups of free groups are free.

Q: How do you recognize if a group $F \in \mathcal{C}$ is free in \mathcal{C} over a subset $G \subseteq F$?

A: Show that G is an independent generating set.

G is a *generating set* for F if $F = \langle G \rangle$.

G is *independent* in F relative to the class \mathcal{C} if every relation $w(\bar{g}) = w'(\bar{g})$ that holds for a tuple of distinct elements in G holds universally in \mathcal{C} . (Every tuple in every member of \mathcal{C} satisfies the relation.)

The fact that F , together with $\iota: G \rightarrow F$, satisfies the universal property of free algebras is readily seen to be equivalent to the property that G is an independent generating set for F .

Schreier's Theorem: Subgroups of free groups are free.

Q: How do you recognize if a group $F \in \mathcal{C}$ is free in \mathcal{C} over a subset $G \subseteq F$?

A: Show that G is an independent generating set.

G is a *generating set* for F if $F = \langle G \rangle$.

G is *independent* in F relative to the class \mathcal{C} if every relation $w(\bar{g}) = w'(\bar{g})$ that holds for a tuple of distinct elements in G holds universally in \mathcal{C} . (Every tuple in every member of \mathcal{C} satisfies the relation.)

The fact that F , together with $\iota: G \rightarrow F$, satisfies the universal property of free algebras is readily seen to be equivalent to the property that G is an independent generating set for F .

That is, “free basis” = “independent generating set”.

Exercise!

Let $F = \mathbb{F}_{\text{Grp}}(x, y)$. Show that $F' = [F, F]$ is free of infinite rank.

Exercise!

Let $F = \mathbb{F}_{\text{Grp}}(x, y)$. Show that $F' = [F, F]$ is free of infinite rank.

Solution:

Exercise!

Let $F = \mathbb{F}_{\text{Grp}}(x, y)$. Show that $F' = [F, F]$ is free of infinite rank.

Solution: Note that for any words $\alpha, \beta \in F$ the commutator $[\alpha, \beta] = \alpha^{-1}\beta^{-1}\alpha\beta$ has total x -degree 0 and total y -degree 0, so the same must be true for every element of $[F, F]$. Conversely, any word with this property is a product of words of the form $[x^m, y^n] = x^{-m}y^{-n}x^m y^n$.

Exercise!

Let $F = \mathbb{F}_{\text{Grp}}(x, y)$. Show that $F' = [F, F]$ is free of infinite rank.

Solution: Note that for any words $\alpha, \beta \in F$ the commutator $[\alpha, \beta] = \alpha^{-1}\beta^{-1}\alpha\beta$ has total x -degree 0 and total y -degree 0, so the same must be true for every element of $[F, F]$. Conversely, any word with this property is a product of words of the form $[x^m, y^n] = x^{-m}y^{-n}x^my^n$. Thus $[F, F]$ is generated by the set $G = \{[x^m, y^n] \mid m, n \in \mathbb{Z}\}$.

Exercise!

Let $F = \mathbb{F}_{\text{Grp}}(x, y)$. Show that $F' = [F, F]$ is free of infinite rank.

Solution: Note that for any words $\alpha, \beta \in F$ the commutator $[\alpha, \beta] = \alpha^{-1}\beta^{-1}\alpha\beta$ has total x -degree 0 and total y -degree 0, so the same must be true for every element of $[F, F]$. Conversely, any word with this property is a product of words of the form $[x^m, y^n] = x^{-m}y^{-n}x^m y^n$. Thus $[F, F]$ is generated by the set $G = \{[x^m, y^n] \mid m, n \in \mathbb{Z}\}$.

To see that G is independent, we must show that any relation $w(\bar{g}) = w'(\bar{g})$ that holds for a tuple of distinct elements in G holds universally.

Exercise!

Let $F = \mathbb{F}_{\text{Grp}}(x, y)$. Show that $F' = [F, F]$ is free of infinite rank.

Solution: Note that for any words $\alpha, \beta \in F$ the commutator $[\alpha, \beta] = \alpha^{-1}\beta^{-1}\alpha\beta$ has total x -degree 0 and total y -degree 0, so the same must be true for every element of $[F, F]$. Conversely, any word with this property is a product of words of the form $[x^m, y^n] = x^{-m}y^{-n}x^m y^n$. Thus $[F, F]$ is generated by the set $G = \{[x^m, y^n] \mid m, n \in \mathbb{Z}\}$.

To see that G is independent, we must show that any relation $w(\bar{g}) = w'(\bar{g})$ that holds for a tuple of distinct elements in G holds universally. It suffices to show that if $g \neq h^{-1} \in G \cup G^{-1}$, then one can determine g and h from an examination of gh . (More specifically, show that g and gh have the same left two blocks when $g \neq h^{-1}$.)