

#### 4. EQUATIONAL LOGIC

Recall that a  $\Sigma$ -equation  $\varepsilon$  is defined to be a logical consequence of a set  $E$  of  $\Sigma$ -equations if every model of  $E$  is a model of  $\varepsilon$ . Thus, taking  $\Sigma$  to be the signature of groups (of type II),  $\varepsilon$  is a law of groups if it is an identity in every group. To establish this fact one obviously cannot consider each group individually and check if  $\varepsilon$  is an identity. A proof is required and it must be a finite process. In the following we define the formal notion of a proof of  $\varepsilon$  from  $E$ ; it is not immediately obviously what is its relation to logical consequence.

**Definition 4.1.** Let  $E$  be a set of  $\Sigma$ -equations. A  $\Sigma$ -equation  $\varepsilon$  is a (*logical*) *consequence* of  $E$ , in symbols  $E \models \varepsilon$ , if every model of  $E$  is a model of  $\varepsilon$ , i.e.,  $\text{Mod}(E) \models \varepsilon$ , that is  $\text{Mod}(E) \subseteq \text{Mod}(\varepsilon)$ .

*Example:* Let  $E$  be the axioms of groups (of type II). Then  $E \models (x \cdot y)^{-1} \approx y^{-1} \cdot x^{-1}$ .

Let  $t$  be a  $\Sigma$ -term. By a *substitution instance* of a  $\Sigma$ -equation  $\varepsilon$  we mean any  $\Sigma$ -equation that is obtained by simultaneously substituting arbitrary  $\Sigma$ -terms for the variables of  $\varepsilon$ . Thus if  $\varepsilon = (t(x_0, \dots, x_{n-1}) \approx s(x_0, \dots, x_{n-1}))$ , then every equation of the form  $t(u_0, \dots, u_{n-1}) \approx s(u_0, \dots, u_{n-1})$ , where  $u_0, \dots, u_{n-1}$  are arbitrary  $\Sigma$ -terms, is a substitution instance of  $\varepsilon$ . A substitution instance of  $x \approx x$  is called a (*logical*) *tautology*. Thus  $u \approx u$  is a tautology for every term  $u$ .

**Definition 4.2.** Let  $E$  be a set of  $\Sigma$ -equations. By an (*equational*) *proof from  $E$*  we mean any finite sequence  $\delta_1, \dots, \delta_m$  of  $\Sigma$ -terms such that, for each  $k \leq m$ , at least one of the following conditions holds.

- (*taut*)  $\delta_k$  is substitution instance of  $x \approx x$ , i.e., a tautology.
- (*E-axiom*)  $\delta_k$  is a substitution instance of an equation in  $E$ .
- (*sym*)  $\varepsilon$  is  $t \approx s$  and there is an  $i < k$  such that  $\delta_i$  is  $s \approx t$ .
- (*trans*)  $\varepsilon_k$  is  $t \approx s$  and there exist  $i, j < k$  such that  $\delta_i$  is  $t \approx r$  and  $\delta_j$  is  $r \approx s$ .
- (*repl*)  $\varepsilon_k$  is of the form  $\sigma(t_0, \dots, t_{n-1}) \approx \sigma(s_0, \dots, s_{n-1})$ , where  $\sigma \in \Sigma_n$  and there are  $i_0, \dots, i_{n-1} < k$  such that  $\delta_{i_0}, \dots, \delta_{i_{n-1}}$  are respectively  $t_0 \approx s_0, \dots, t_{n-1} \approx s_{n-1}$ .

The five conditions that define an equational proof are called *rules*. Each of the first two, (*taut*) and (*E-axiom*), is called an *axiom* because it allows one to introduce an equation in the proof independently of any particular equation or equations occurring earlier in the proof. The last three, (*sym*), (*trans*), and (*repl*) are called *inference rules*. The equation that each of them introduces into the proof is called the *conclusion* of the rule; the equation(s) occurring earlier in the proof that justify the conclusion are called *premisses*.

Traditionally axioms and inference rules are represented by drawing a horizontal line between the premisses and the conclusion. We summarize the axioms and rules of inference symbolically in this form below.

In the following  $r, s, s_0, s_1, \dots, t, t_0, t_1, \dots, u_0, \dots, u_{n-1}$  represent arbitrary  $\Sigma$ -terms and  $E$  an arbitrary set of  $\Sigma$ -equations.

- (*taut*)  $t \approx t$ .
- (*E-axiom*)  $t(u_0, \dots, u_{n-1}) \approx s(u_0, \dots, u_{n-1})$ ,  
for each  $t(x_0, \dots, x_{n-1}) \approx s(x_0, \dots, x_{n-1})$  in  $E$ .

$$\begin{aligned}
(\text{sym}) \quad & \frac{t \approx s}{s \approx t}. \\
(\text{trans}) \quad & \frac{t \approx r, r \approx s}{t \approx s}. \\
(\text{repl}) \quad & \frac{t_0 \approx s_0, \dots, t_{n-1} \approx s_{n-1}}{\sigma(t_0, \dots, t_{n-1}) \approx \sigma(s_0, \dots, s_{n-1})}, \quad \text{for each } \sigma \in \Sigma_n.
\end{aligned}$$

**Definition 4.3.** Let  $E$  be a set of  $\Sigma$ -equations. A  $\Sigma$ -equation  $\varepsilon$  is (*equationally*) *provable* from  $E$ , in symbols  $E \vdash \varepsilon$ , if there is a proof  $\delta_1, \dots, \delta_m$  from  $E$  such that the last equation  $\delta_m$  is  $\varepsilon$ .

*Example:* As an example we construct an equational proof of  $(x \cdot y)^{-1} \approx y^{-1} \cdot x^{-1}$  from the axioms of group theory. We first prove it informally, the way it would be done in an algebra course, and then show how to convert this into a formal equational proof.

The most natural way to prove it is to use the fact that in a group the inverse of each element is unique. Assume  $xy = e$ ; as usual we omit the multiplication symbol “ $\cdot$ ” when write products informally.

$$(29) \quad (xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e.$$

So by the uniqueness of the inverse, we have  $(xy)^{-1} = y^{-1}x^{-1}$ . The formal equational proof must incorporate the proof of the fact that the inverse is unique. Here is its informal proof: Assume  $xy = e$ . Then

$$(30) \quad y = ey = (x^{-1}x)y = x^{-1}(xy) = x^{-1}e = x^{-1}.$$

Note that all the steps in this proof follow from the axioms of group theory except for the next-to-last equality; this uses the assumption that  $xy = e$ . We now transform (30) into an informal proof of  $(x \cdot y)^{-1} \approx y^{-1} \cdot x^{-1}$  by substituting “ $(xy)$ ” for all occurrences of “ $x$ ” and “ $(y^{-1}x^{-1})$ ” for all occurrences of “ $y$ ”. Note that under these substitutions the next-to-last equality of the transformed proof becomes “ $(xy)^{-1}((xy)(y^{-1}x^{-1})) = (xy)^{-1}e$ ”, which is obtained from a substitution instance of the assumption “ $xy = e$ ” by replacement. This next-to-last equality in the transformed proof (30) is then expanded into a series of steps by incorporating the proof of  $(xy)(y^{-1}x^{-1}) = e$  given in (29). This gives an informal of  $(x \cdot y)^{-1} \approx y^{-1} \cdot x^{-1}$  directly from the axioms of group theory. Here it is.

$$\begin{aligned}
(31) \quad y^{-1}x^{-1} &= e(y^{-1}x^{-1}) = (xy^{-1}(xy))(y^{-1}x^{-1}) = (xy)^{-1}((xy)(y^{-1}x^{-1})) \\
&= (xy)^{-1}((x(yy^{-1}))x^{-1}) = (xy)^{-1}((xe)x^{-1}) = (xy)^{-1}(xx^{-1}) = (xy)^{-1}e = (xy)^{-1}.
\end{aligned}$$

This informal proof appears to use only the axioms of groups, but it also implicitly uses properties of equality. For example, that we can write it as a long sequence of terms separated by equality symbols, rather than a sequence of individual equations, implicitly uses the transitivity of equality. In a formal equational proof each use of a property of equality must be justified by an axiom or rule of equality, i.e., by (*taut*) or by one of the inference rules (*sym*), (*trans*), or (*repl*). In Figure 22 we give a fragment of the formal equational proof of  $(x \cdot y)^{-1} \approx y^{-1} \cdot x^{-1}$  from the axioms  $E$  of groups—the part that terminates in a proof  $y^{-1} \cdot x^{-1} \approx ((x \cdot y)^{-1} \cdot (x \cdot y)) \cdot (y^{-1} \cdot x^{-1})$ .

We now clarify the relation between the semantical relation of logical consequence  $\models$  and that of equational proof  $\vdash$ ; we see that these conceptionally very different notions give the same abstract relation.

1.  $e \cdot (y^{-1} \cdot x^{-1}) \approx y^{-1} \cdot x^{-1}$  (*E-axiom*), subst. inst. of  $e \cdot x \approx x$
2.  $y^{-1} \cdot x^{-1} \approx e \cdot (y^{-1} \cdot x^{-1})$  1, (*sym*)
3.  $(x \cdot y)^{-1} \cdot (x \cdot y) \approx e$  (*E-axiom*), subst. inst. of  $x \cdot x^{-1} \approx e$
4.  $e \approx (x \cdot y)^{-1} \cdot (x \cdot y)$  3, (*sym*)
5.  $y^{-1} \cdot x^{-1} \approx y^{-1} \cdot x^{-1}$  (*taut*)
6.  $e \cdot (y^{-1} \cdot x^{-1}) \approx ((x \cdot y)^{-1} \cdot (x \cdot y)) \cdot (y^{-1} \cdot x^{-1})$  4,5, (*repl*)
7.  $y^{-1} \cdot x^{-1} \approx ((x \cdot y)^{-1} \cdot (x \cdot y)) \cdot (y^{-1} \cdot x^{-1})$  2,6, (*trans*)

FIGURE 22

**Theorem 4.4** (Soundness Theorem for Equational Logic). *For any set  $E \cup \{\varepsilon\}$  of  $\Sigma$ -equations, if  $\varepsilon$  is equationally provable from  $E$  then it is a logical consequence of  $E$ , i.e.,  $E \vdash \varepsilon$  implies  $E \models \varepsilon$ .*

*Proof.* Assume  $E \vdash \varepsilon$ . Let  $\delta_1, \dots, \delta_m$  with  $\delta_m = \varepsilon$  be an equational proof of  $\varepsilon$  from  $E$ . We prove that  $E \models \delta_k$  for all  $k \leq m$  by induction on  $k$ .

Let  $\hat{v} = \langle x_0, \dots, x_{n-1} \rangle$  include every variable occurring in at least one of the  $\delta_k$ . Assume  $\delta_k$  is of the form  $t_k(\hat{x}) \approx s_k(\hat{x})$  for every  $k \leq m$ . Recall that  $E \models \delta_k$  means that, for every  $\mathbf{A} \in \text{Mod}(E)$  and every  $\hat{a} = \langle a_0, \dots, a_{n-1} \rangle \in A^n$ ,  $t_k^{\mathbf{A}}(\hat{a}) = s_k^{\mathbf{A}}(\hat{a})$ . Let  $\mathbf{A} \in \text{Mod}(E)$  and  $\hat{a} \in A^n$  be fixed but arbitrary.

For  $k = 1$ ,  $\delta_1$  must be either a tautology or a substitution instance of an equation in  $E$ , i.e.,  $\delta_1$  is in one of the two following forms:  $u(\hat{x}) \approx u(\hat{x})$  or

$$u(w_0(\hat{x}), \dots, w_{l-1}(\hat{x})) \approx v(w_0(\hat{x}), \dots, w_{l-1}(\hat{x})) \quad \text{where } u(y_0, \dots, y_{l-1}) \approx v(y_0, \dots, y_{l-1}) \text{ is in } E.$$

In the first case  $t_1^{\mathbf{A}}(\hat{a}) = u^{\mathbf{A}}(\hat{a}) = u^{\mathbf{A}}(\hat{a}) = s_1^{\mathbf{A}}(\hat{a})$ . In the second case, by assumption we have that  $u^{\mathbf{A}}(\hat{b}) = v^{\mathbf{A}}(\hat{b})$  for all  $\hat{b} \in A^l$ . Thus

$$t_1^{\mathbf{A}}(\hat{a}) = u^{\mathbf{A}}(\underbrace{w_0^{\mathbf{A}}(\hat{a})}_{b_0}, \dots, \underbrace{w_{l-1}^{\mathbf{A}}(\hat{a})}_{b_{l-1}}) = v^{\mathbf{A}}(\underbrace{w_0^{\mathbf{A}}(\hat{a})}_{b_0}, \dots, \underbrace{w_{l-1}^{\mathbf{A}}(\hat{a})}_{b_{l-1}}) = s_1^{\mathbf{A}}(\hat{a}).$$

Suppose  $k > 1$ . If  $\varepsilon_k$  is a tautology or substitution instance of an equation of  $E$  we proceed as above. So we can assume that  $\varepsilon_k$  is obtained from earlier equations in the proof by one of the inference rules.

Consider (*repl*). Suppose

$$\varepsilon_k = \left( \underbrace{\sigma(t_{i_1}(\hat{x}), \dots, t_{i_m}(\hat{x}))}_{t_k(\hat{x})} \approx \underbrace{\sigma(s_{i_1}(\hat{x}), \dots, s_{i_m}(\hat{x}))}_{s_k(\hat{x})} \right),$$

where  $i_1, \dots, i_m < k$ . By the induction hypothesis  $E \models \underbrace{t_{i_j}(\hat{x}) \approx s_{i_j}(\hat{x})}_{\delta_{i_j}}$  for all  $j \leq m$ . Thus

$t_{i_j}^{\mathbf{A}}(\hat{a}) = s_{i_j}^{\mathbf{A}}(\hat{a})$  for  $j \leq m$ , and hence

$$t_k^{\mathbf{A}}(\hat{a}) = \sigma^{\mathbf{A}}(t_{i_1}^{\mathbf{A}}(\hat{a}), \dots, t_{i_m}^{\mathbf{A}}(\hat{a})) = \sigma^{\mathbf{A}}(s_{i_1}^{\mathbf{A}}(\hat{a}), \dots, s_{i_m}^{\mathbf{A}}(\hat{a})) = s_k^{\mathbf{A}}(\hat{a}).$$

Hence  $E \models \delta_k$ .

The rules (*sym*) and (*trans*) are left as exercises.  $\square$

Sometimes the following rule of substitution is included among the rules of equational logic.

$$(sub) \frac{t(x_0, \dots, x_{n-1}) \approx s(x_0, \dots, x_{n-1})}{t(u_0, \dots, u_{n-1}) \approx s(u_0, \dots, u_{n-1})}, \text{ for all } u_0, \dots, u_{n-1} \in \text{Te}_\Sigma(X).$$

The next lemma shows that the rule would be redundant—every equation that is provable with it is provable without it.

**Lemma 4.5.** *For any set of  $\Sigma$ -equations  $E \cup \{t(x_0, \dots, x_{n-1}) \approx s(x_0, \dots, x_{n-1})\}$  and any sequence  $u_0, \dots, u_{n-1}$  of  $\Sigma$ -terms we have that  $E \vdash t(x_0, \dots, x_{n-1}) \approx s(x_0, \dots, x_{n-1})$  implies  $E \vdash t(u_0, \dots, u_{n-1}) \approx s(u_0, \dots, u_{n-1})$ , i.e., every substitution instance of an equation provable from  $E$  is itself provable from  $E$ .*

The proof is left as an exercise. It goes by induction on the length of proofs. Note that the base step is guaranteed by the fact that by (*E-axiom*) every substitution instance of an equation of  $E$  is automatically provable from  $E$ .

*Problem:* Suppose you are asked by your algebra instructor either to prove that every Boolean group is Abelian or to find a counterexample (a *Boolean group* is a group in which every nonidentity is of order 2). What does this mean? Let  $E$  be the axioms of groups. Then you are asked to verify either

$$E \cup \{x \cdot x \approx e\} \vdash x \cdot y \approx y \cdot x \quad \text{or} \quad E \cup \{x \cdot x \approx e\} \not\vdash x \cdot y \approx y \cdot x.$$

But why do you know that at least one of these two alternatives must be true? That is, how can you be sure that if  $x \cdot y \approx y \cdot x$  is not provable from the axioms of groups together with  $x \cdot x \approx e$ , then a counterexample must exist? Formally, does

$$E \cup \{x \cdot x \approx e\} \not\vdash x \cdot y \approx y \cdot x \quad \text{imply} \quad E \cup \{x \cdot x \approx e\} \not\vdash x \cdot y \approx y \cdot x?$$

This implication, in its contrapositive form, is the completeness theorem of equational logic. The completeness theorem can be paraphrased as “If an equation is not provable there must be a counterexample.”

**Theorem 4.6** (Completeness Theorem of Equational Logic). *For any set  $E \cup \{\varepsilon\}$  of  $\Sigma$ -equations, if  $\varepsilon$  is a logical consequence of  $E$ , then  $\varepsilon$  is equationally provable from  $E$ , i.e.,*

$$E \models \varepsilon \quad \text{implies} \quad E \vdash \varepsilon.$$

*Proof.* We prove the contrapositive, i.e., from the assumption that  $\varepsilon$  is not provable from  $E$  we construct a  $\Sigma$ -algebra  $\mathbf{A}$  such that  $\mathbf{A} \in \text{Mod}(E)$  but  $\mathbf{A} \notin \text{Mod}(\varepsilon)$ .

Let  $\alpha = \{\langle t, s \rangle \in \text{Te}_\Sigma(X)^2 : E \vdash t \approx s\}$ .

**Claim.**  $\alpha \in \text{Co}(\text{Te}_\Sigma(X))$ .

*Proof of claim.* By (*taut*),  $E \vdash t \approx t$  and hence  $\langle t, t \rangle \in \alpha$  for every  $t \in \text{Te}_\Sigma(X)$ , i.e.,  $\alpha$  is reflexive.

$$\langle t, s \rangle \in \alpha \implies E \vdash t \approx s \xRightarrow{(sym)} E \vdash s \approx t \implies \langle t, s \rangle \in \alpha.$$

So  $\alpha$  is symmetric.

$$\langle t, r \rangle, \langle r, s \rangle \in \alpha \implies E \vdash t \approx r, r \approx s \xRightarrow{(trans)} E \vdash t \approx s \implies \langle t, s \rangle \in \alpha.$$

So  $\alpha$  is transitive. For any  $\sigma \in \Sigma_n$ ,

$$\begin{aligned} \langle t_1, s_1 \rangle, \dots, \langle t_n, s_n \rangle \in \alpha &\implies E \vdash t_1 \approx s_1, \dots, t_n \approx s_n \\ &\implies \vdash \sigma(t_1, \dots, t_n) \approx \sigma(s_1, \dots, s_n) \\ &\quad \text{(repl)} \\ &\implies \langle \sigma(t_1, \dots, t_n), \sigma(s_1, \dots, s_n) \rangle \in \alpha. \end{aligned}$$

So  $\alpha$  has the substitution property. □ claim.

Let  $\mathbf{A} = \mathbf{Te}_\Sigma(X)/\alpha$ .

**Claim.**  $\mathbf{A} \in \text{Mod}(E)$ .

*Proof of claim.* Let  $t(\hat{x}) \approx s(\hat{x})$  be in  $E$ , with  $\hat{x} = \langle x_0, \dots, x_{n-1} \rangle$ . Let  $\hat{a} = \langle a_0, \dots, a_{n-1} \rangle \in A^n$ . We must show that  $t^{\mathbf{A}}(\hat{a}) = s^{\mathbf{A}}(\hat{a})$ . Let  $\hat{u} = u_0, \dots, u_{n-1} \in \mathbf{Te}_\Sigma(X)^n$  such that  $a_i = u_i/\alpha$  for all  $i < n$ . Then

$$\begin{aligned} t^{\mathbf{A}}(\hat{a}) &= t^{\mathbf{Te}_\Sigma(X)/\alpha}(u_0/\alpha, \dots, u_{n-1}/\alpha) = t(\hat{u})/\alpha, \quad \text{and} \\ s^{\mathbf{A}}(\hat{a}) &= s^{\mathbf{Te}_\Sigma(X)/\alpha}(u_0/\alpha, \dots, u_{n-1}/\alpha) = s(\hat{u})/\alpha. \end{aligned}$$

But  $E \vdash t(\hat{u}) \approx s(\hat{u})$  by (*E-axiom*). So  $\langle t(\hat{u}), s(\hat{u}) \rangle \in \alpha$ , i.e.,  $t(\hat{u})/\alpha = s(\hat{u})/\alpha$ . □ claim.

**Claim.**  $\mathbf{A} \notin \text{Mod}(\varepsilon)$ .

*Proof of claim.* Let  $\varepsilon$  be  $t(\hat{x}) \approx s(\hat{x})$  with  $\hat{x} = \langle x_0, \dots, x_{n-1} \rangle$ . Must show there exist  $\hat{a} = \langle a_0, \dots, a_{n-1} \rangle \in A^n$  such that  $t^{\mathbf{A}}(\hat{a}) \neq s^{\mathbf{A}}(\hat{a})$ .

Let  $a_i = x_i/\alpha$  for each  $i < n$ . Then  $t^{\mathbf{A}}(\hat{a}) = t(\hat{x})/\alpha$  and  $s^{\mathbf{A}}(\hat{a}) = s(\hat{x})/\alpha$ . But  $\langle t(\hat{x}), s(\hat{x}) \rangle \notin \alpha$  since  $E \not\vdash \varepsilon$  by assumption. So  $t^{\mathbf{A}}(\hat{a}) \neq s^{\mathbf{A}}(\hat{a})$ . □ claim.

Thus by the two claims  $E \not\vdash \varepsilon$ . □