6.11. The word problem.

Let Γ be a group with finite generating set S.
Let $W(S \cup S^{-1})$ be the set of words in S and their (formal) inverses.

Definition : We say that Γ has soluble word problem if there is an algorithm to decide if a given $w \in W$ represents the trivial word.

Note: this is independent of the choice of finite generating set S.

Remarks.
(1) The algorithm is only required to return "yes" or "no". It's not required to justify its answer.
(2) Also, we are not asked for a general procedure that can take any group presentation an produce algorithm. For any given group, it is enough to just to produce one out of thin air.

We aim to show that any hyperbolic group has soluble word problem.

Let Γ be a hyperbolic group, and let S be any generating set. Write $W \in W(S \sqcup S^{-1})$. Let $p : W \longrightarrow \Gamma$ be the natural map.

Lemma 6.21 : *There is some $n \in \mathbf{N}$ such that if $w \in W(S \sqcup S^{-1})$ is a non-empty word of length at least n and with $p(w) = 1$, then there is a subword, v, of w of length n, and another word $u \in W$, of length less than n, with $p(u) = p(v)$.*

Proof : Set l sufficiently large, as below, and set $n = 2l$. Let Δ be the Cayley graph. Let γ be the path representing w in Δ. Since $p(w) = 1$ this is closed. Suppose the conclusion fails. Then every subpath of γ of length n is geodesic.

Let z be a furthest point from 1 in γ, i.e. with $r = d(1, z)$ maximal. Let $\beta \subseteq \gamma$ be the arc of length $2l$ centred on z, and let x, y be its endpoints. Note that $1 \notin \beta$ (otherwise, $d(1, z)$ could not have been maximal).

Now $d(x, z) = d(y, z) = l$, $d(x, y) = 2l$, $d(1, x) \leq r$ and $d(1, y) \leq r$. Thus

$$\begin{aligned} d(1, z) + d(x, y) &= r + 2l \\ d(1, x) + d(y, z) &\leq r + l \\ d(1, y) + d(x, z) &\leq r + l. \end{aligned}$$

By the four point condition of hyperbolicity, the largest two of these quantities are within k' of each other. Thus, $l \leq k'$. Setting $l = k' + 1$, we therefore get a contradiction. $\diamondsuit$

Corollary 6.21 : *A hyperbolic group has soluble word problem.*

Proof : Let $W_0 \subseteq W$ be the list of all words of length at most $2n$ with $p(w) = 1$. This set is finite.

We are given $w \in W$. If w has length at most n, check to see if $w \in W_0$, and return "yes" or "no" accordingly. In it has length greater than n, we look for a subword v, of length n in W, and a word $u \in W$, of length less than n, with $vu^{-1} \in W_0$. In none exists, return "no". If we find such v, u, replace v by u in w and go back to the begning. Note that we have reduced the length of w so the process must terminate.

To see this works, apply Lemma 2.21. $\diamondsuit$

Remarks.

(1) It's enough that our algorithm should return "yes" or "no". It doesn't have to justify itself. However, the argument shows that in this particular case, the machine is capable of doing more: namely generating an explicit proof that it is correct.

(2) The set W_0 forms part the machine. We know that it exists. We don't need to know how to find it.

In fact (though this requires more work) there is an explicit algorithm that takes a group presentation, and produces such a set W_0 if the group is hyperbolic. (If the group is not hyperbolic, the process might not terminate.)