1 Introduction

The purpose of this work is to give a detailed proof for an exercise which appears in "A Course in the Theory of Groups, second edition" by Derek Robinson, [ROB] from now on. The exercise appears on page 50 of the book and goes as follows:

1.

> If F is a free group on a subset X and $\emptyset \neq Y \subset X$, prove that F/Y^F is free on $X \setminus Y$.

I'm assuming here that the reader is already familiar with some basic definitions and facts about free groups (and groups in general) although I give further down some of the precise definitions I will be using. "subset X" is probably a typo and what was meant was "set X". In the above the only notation which is not totally standard if Y^F which [ROB] calls the *normal closure* of Y in F and defines as follows:

2. Definition: For a group F and any $Y \subseteq F$, the normal closure of Y in F (in notation, Y^F) is the least normal subgroup of F which contains Y.

So the exercise wants us to prove that the free group generated by $X \setminus Y$, lets call it for now F', is isomorphic to the quotient group F/Y^F. No hint is given.

It seems obvious that the intended isomorphism is the one which sends a word $x \in F'$ to $x \cdot Y^F$. Proving that this is onto is easy enough. But how to prove that it is 1-1? The only way I can think of is to prove a certain intermediate result. Before I get to that, I need to fix the definition of a free group. For this, I find the technicalities more convenient if I follow the construction of a free group given in "Algebra" by Pierre Grillet ([GRI] from now on) rather than the one in [ROB]. So now I will summarise the construction. For all the details, the reader should consult any of the 2 books.

3. Start with a non empty set X. Fix a set X' with the same cardinality as X so that $X \cap X' = \emptyset$ and fix a bijection from X to X'. For every $x \in X$, the image of x through the bijection will be denoted as x^{-1} and for every $x' \in X'$, the inverse image of x' through the bijection will be denoted as x'^{-1}. So in particular we have that for every $x \in X \cup X'$, $(x^{-1})^{-1} = x$. Let $\overline{X} = X \cup X'$. We consider formal products of elements of $\overline{X}$ i.e. finite sequences of elements of $\overline{X}$. Such finite sequences, including the empty one, will be called *words* (over $\overline{X}$). We will denote the set of all such words by

$\mathbb{W}$ or $\mathbb{W}(T)$ if we want to refer to some set other than X. Formally, every $w \in \mathbb{W}$ is a function from some $n \in \mathbb{N}$ to $\overline{X}$. The domain of w (i.e. this n) will be denoted by $\text{len}(w)$.

4. We define a product on $\mathbb{W}$: for all w_1, w_2, $w_1 \odot w_2$ will be the concatenation of w_1 and w_2. Obviously, $\text{len}(w_1 \odot w_2) = \text{len}(w_1) + \text{len}(w_2)$.

A $w \in \mathbb{W}$ will be called *reduced* if there is no $i \in \text{len}(w)$ such that $i+1 \in \text{len}(w)$ and $w(i+1) = w(i)^{-1}$. ("reduced" is standard terminology. Why not "irreducible" like with polynomials? I don't know, perhaps for variety) On the other hand, if such an i does exist then we say that a *cancellation* ([GRI] calls it *"one-step reduction"*) is possible which is gives the $w' \in \mathbb{W}$ with domain $\text{len}(w) - 2$ which is defined as $w'(j) = w(j)$ if $j < i$ and $w'(j) = w(j+2)$ if $j >= i$.

Obviously, starting with any $w \in \mathbb{W}$, after a finite number of cancellations we will arrive at a reduced $w' \in \mathbb{W}$. For the construction of the free group the following result is crucial:

5. Proposition: For every $w \in \mathbb{W}$, there is a unique reduced $w' \in \mathbb{W}$ which is obtained by a sequence of cancellations from w. In other words, regardless of the order in which we carry out any cancellations from w, we will always arrive at the same reduced w'. This unique w' will be denoted as $\mathfrak{r}(w)$.

Both [ROB] and [GRI] give a proof of the result and it's not hard to do as an exercise; it certainly strikes me as easier than the exercise in [ROB] which this work is about. [ROB] defines an equivalence relation on the set of all words as $w_1 \sim w_2$ iff $\mathfrak{r}(w_1) = \mathfrak{r}(w_2)$ (this isn't his actual definition but it amounts to this) and the free group as the set of equivalence classes. This is a bit awkward for my purposes so I will follow the definition in [GRI] where the free group is the set of reduced words with the product defined as $w_1 \cdot w_2 = \mathfrak{r}(w_1 \odot w_2)$. It's trivial to show that the two definitions give isomorphic groups. I will denote the free group over X by $\mathbb{F}$ and, if I need to refer to a different set T, by $\mathbb{F}(T)$.

We identify $\overline{X}$ with the set of words of length 1. This way every $T \subseteq X$ defines a subset of $\mathbb{F}$ and $\mathbb{F}(T)$ can be taken to be the subgroup of $\mathbb{F}$ generated by T. From now on I will use G_1 to refer to $\mathbb{F}(X \setminus Y)$ where Y is as it appears in ¶1; I will use N to refer to the least normal subgroup of $\mathbb{F}$ which contains Y. So the exercise in [ROB] wants us to prove that

6. Proposition: G_1 is isomorphic to $\mathbb{F}/N$.

We set $\overline{Y} = Y \cup Y^{-1}$. It's easy to see that $\overline{X} \setminus \overline{Y} = (X \setminus Y) \cup (X \setminus Y)^{-1}$. Now I will state the "intermediate result" I mentioned earlier:

7. Proposition: for every $x \in N$, if $\text{len}(x) > 0$ (i.e. if x is not the identity) then there exists some $i \in \text{len}(x)$ such that $x(i) \in \overline{Y}$.

From now on I will denote by H the homomorphism which sends every $x \in G_1$ to $x \cdot N \in \mathbb{F}/N$.

8. Proposition: H is onto; assuming proposition 7, H is also 1-1.
Proof: For the onto part it suffices to show that for every $x \in \mathbb{F}$ there exists some $x_1 \in G_1$ such that $x_1 \cdot N = x \cdot N$ which is equivalent to $x_1^{-1} \cdot x \in N$. We use induction on $\text{len}(x)$. Assume it holds for every $x' \in \mathbb{F}$ with $\text{len}(x') = n$ and assume that $\text{len}(x) = n + 1$. Let $x_2 \in G_1$ be such that $x_2^{-1} \cdot x|_n \in N$. Let $t = x(n)$.

If $t \in \overline{Y}$ then $x_2^{-1} \cdot x = (x_2^{-1} \cdot x|_n) \cdot t \in N \cdot t = N$.

If $t \notin \overline{Y}$ then $t \in G_1 \Rightarrow x_2 \cdot t \in G_1$ and, because N is normal, $t^{-1} \cdot x_2^{-1} \cdot x|_n \cdot t \in N \Rightarrow t^{-1} \cdot x_2^{-1} \cdot x \in N \Rightarrow (x_2 \cdot t)^{-1} \cdot x \in N$.

Now assume proposition 7. Let $x_1, x_2 \in G_1$ be such that $x_1 \cdot N = x_2 \cdot N \Rightarrow x_2^{-1} \cdot x_1 \in N$. If $x_2^{-1} \cdot x_1 \neq \imath$ then there exists some $i \in \text{len}(x_2^{-1} \cdot x_1)$ such that $(x_2^{-1} \cdot x_1)(i) \in \overline{Y}$. But this is impossible because x_1 and x_2 are sequences which only have elements from $(X \setminus Y) \cup (X \setminus Y)^{-1} = \overline{X} \setminus \overline{Y}$.
□

So now the sticky part is to prove proposition 7. Note that if we just wanted the result for the least subgroup of $\mathbb{F}$ which contains Y then it would be trivial. But a normal subgroup N' must also be closed under products of the form $t^{-1} \cdot x \cdot t$ for all $t \in \mathbb{F}$ and $x \in N'$. On first look one cannot exclude the possibility that there is some clever way to arrange products of this sort in a way which ends up with a non empty sequence which is an element of N and contains no element from $\overline{Y}$. It could be that there exists some much more straightforward proof than what I have been able to find or it could be that Robinson considered the result intuitively obvious and in no need of a proof or it could be that he underestimated the difficulty of proving it. Towards the end of this work I will present a more direct approach. It works for some simple cases but I didn't manage to make it work for more complicated ones so I had to adopt a different line of attack.

2 Main course

9. Definitions: FS will denote the set of all finite subsets of $\mathbb{N}$; for $A \in \text{FS}$, $\text{card}(A)$ will be the size of A. For A, B in FS with the same size, $\text{SI}(A, B)$ will mean the unique strictly increasing function from A to B. A *generalised word* is a function from some $A \in \text{FS}$ to $\overline{X}$ and the set of all generalised

words will be denoted by $\mathbb{GW}$. For any $x \in \mathbb{GW}$, $\text{dom}(x)$ is the domain of x i.e. the set in FS on which x is defined. If $x \in \mathbb{GW}$ with $A = \text{dom}(x)$ and for any $B \in \text{FS}$ with $\text{card}(A) = \text{card}(B)$, the *transfer* of x from A to B, in notation $\text{tr}(x, A, B)$, is defined as $\text{tr}(x, A, B) = x \circ \text{SI}(B, A)$. Obviously $\text{tr}(x, A, B) \in \mathbb{GW}$ and $\text{dom}(\text{tr}(x, A, B)) = B$. In particular, for all $x \in \mathbb{GW}$, $\text{tr}(x, \text{dom}(x), \text{card}(\text{dom}(x))) \in \mathbb{W}$. If for some $x \in \mathbb{GW}$ there exist $i_1, i_2 \in \text{dom}(x)$ such that $i_1 < i_2$ and there is no $j \in \text{dom}(x)$ with $i_1 < j < i_2$ and $x(i_2) = x(i_1)^{-1}$ then a *cancellation* is possible which gives a new element of $\mathbb{GW}$ which is the restriction of x to the set $\text{dom}(x) \setminus \{i_1, i_2\}$. x will be called *reduced* if no cancellations are possible.

After the above niggling technicalities, we arrive at a more interesting definition:

10. Definitions: For every $x \in \mathbb{GW}$ the *support* of x, in notation $\text{su}(x)$, is the set $\{i \in \text{dom}(x) : x(i) \notin \overline{Y}\}$. A *good pairing* (GP) on x is an equivalence relation on $\text{su}(x)$ which satisfies the following properties:

GP1: Every equivalence class has size 2.
GP2: If $\{i_1, i_2\}, \{j_1, j_2\}$ are equivalence classes with $i_1 < j_1 < i_2$ then $i_1 < j_2 < i_2$; so equivalence classes are "nested" in a certain way.
GP3: If $\{i_1, i_2\}$ is an equivalence class then $x(i_2) = x(i_1)^{-1}$.
GP4: If $\{i_1, i_2\}$ is an equivalence class with $i_1 < i_2$ then there exists a $j \in \text{dom}(x)$ with $i_1 < j < i_2$ and $j \notin \text{su}(x)$.

For the avoidance of doubt, if $\text{su}(x) = \emptyset$ then x is considered to have a good pairing. If P is an equivalence relation which is a GP and $i \in \text{su}(x)$ then $P(i)$ will denote the unique $j \in \text{su}(x)$ such that $\{i, j\}$ is an equivalence class. The notation I will be using for GPs will be as a set of equivalence classes rather than as a set of ordered pairs.

11. Proposition: Let $x \in \mathbb{GW}$ be not reduced and assume that there exists a GP P on x. Then it is possible to perform a sequence of cancellations starting from x in such a way that the $x' \in \mathbb{GW}$ we reach at the end will also admit a GP P'.
Proof: For the rest of the proof we fix $i_0, i'_0 \in \text{dom}(x)$ such that $i_0 < i'_0$ and $x(i'_0) = x(i_0)^{-1}$ and there is no $i \in \text{dom}(x)$ with $i_0 < i < i'_0$. Note that $x(i'_0) = x(i_0)^{-1}$ implies that $i_0 \in \text{su}(x) \Leftrightarrow i'_0 \in \text{su}(x)$.

The notation $i \approx j$ will mean that $i, j \in \text{dom}(x)$, $i \neq j$ and there is no $i_1 \in \text{dom}(x)$ which is between i and j. So we have $i_0 \approx i'_0$. Note that if $i, j \in \text{su}(x)$ and $i \approx j$ then GP4 implies that $\{i, j\}$ is not an equivalence class of P.

Case 1: $i_0 \in \text{su}(x)$.

From GP3 we have that $x(P(i_0)) = x(i_0)^{-1} = x(i'_0) = x(P(i'_0))^{-1}$.

Case 1.1: $i_0 < P(i_0)$. From the assumptions that $i_0 < i'_0$, $i_0 \approx i'_0$ and GP2 it follows that $i_0 < i'_0 < P(i'_0) < P(i_0)$.

Case 1.1.1: $P(i_0) \approx P(i'_0)$. This implies that a cancellation between $x(P(i_0))$ and $x(P(i'_0))$ is also possible. So we do the cancellations between $x(i_0)$ and $x(i'_0)$ and $x(P(i_0))$ and $x(P(i'_0))$ and we obtain $x' \in \mathbb{GW}$ with

$$\mathrm{dom}(x') = \mathrm{dom}(x) \setminus \{i_0, i'_0, P(i_0), P(i'_0)\}$$

and

$$P' = P \setminus \{\{i_0, P(i_0)\}, \{i'_0, P(i'_0)\}\}$$

It is mechanical to check that P' satisfies GP1-GP4.

Case 1.1.2: It does not hold that $P(i_0) \approx P(i'_0)$. We want to prove that there exists a $j_0 \in \mathrm{dom}(x)$ such that $P(i'_0) < j_0 < P(i_0)$ and $j_0 \notin \mathrm{su}(x)$. Take some $i_1 \in \mathrm{dom}(x)$ with $P(i'_0) < i_1 < P(i_0)$. If $i_1 \notin \mathrm{su}(x)$, we're done. Otherwise it is also the case that $P(i'_0) < P(i_1) < P(i_0)$ because every other possibility leads to a contradiction using GP2. Then GP4 gives us the j_0 we want.

We define x' to be the restriction of x to the set

$$\mathrm{dom}(x) \setminus \{i_0, i'_0\}$$

and

$$P' = (P \setminus \{\{i_0, P(i_0)\}, \{i'_0, P(i'_0)\}\}) \cup \{P(i_0), P(i'_0)\}$$

It is mechanical to check that P' satisfies GP1-GP4; in particular j_0 ensures that GP4 is satisfied.

Case 1.2: $P(i_0) < i_0$.

Case 1.2.1: $P(i'_0) < i'_0$ which implies that $P(i'_0) < P(i_0) < i_0 < i'_0$.

Case 1.2.1.1: $P(i_0) \approx P(i'_0)$. This is the symmetrical of case 1.1.1 and x' and P' are defined in the same manner.

Case 1.2.1.2: It does not hold that $P(i_0) \approx P(i'_0)$. This is the symmetrical of case 1.1.2 and x' and P' are defined in the same manner.

Case 1.2.2: $i'_0 < P(i'_0)$. x' and P' are defined as in case 1.1.2.

Case 2: $i_0 \notin \mathrm{su}(x)$. Let $n = \mathrm{card}(\mathrm{dom}(x))$ and $f = \mathrm{SI}(\mathrm{dom}(x), n)$. Let $A = \{i \in \mathrm{dom}(x) : i < i_0$ and for all $i_1 \in \mathrm{dom}(x)$, $\Big(i \leq i_1 < i_0 \Rightarrow \big(i_1 \in \mathrm{su}(x)$ and $f(i_0) - f(i_1) = f(P(i_1)) - f(i'_0)\big)\Big)$.

I will give here a specific example to help the reader visualise what's happening. Assume for a moment that $x = \langle y_0, y_1, y_2, y_3, y_3^{-1}, y_2^{-1}, y_1^{-1}, y_4, y_0^{-1}\rangle$. So $\mathrm{dom}(x) = n = 9$. Assume that $\mathrm{su}(x) = \{0, 1, 2, 5, 6, 8\}$. If we set $P = \{\{0, 8\}, \{1, 6\}, \{2, 5\}\}$, it is a GP. Let $i_0 = 3$ and $i'_0 = 4$. Then $A = \{1, 2\}$. With all this in place, note that if we simply cancel out y_3 with y_3^{-1} then the 2 elements of the equivalence class $\{2, 5\}$ will be next to each other (i.e. $2 \approx 5$) so GP4 will no longer be true. So then we must also cancel out $x(2)$ with $x(5)$ and finally $x(1)$ with $x(6)$.

This should make clear the gist of things. So now we can return to the proof.

Case 2.1: A is not empty and let i_3 be its least element. This means that $A = \{i \in \mathrm{dom}(x) : i_3 \le i < i_0\}$. Let $j_3 = f(i_3)$ and $j_0 = f(i_0)$. We do in sequence the cancellations $x(i_0)$ with $x(i'_0)$ and then $x(f^{-1}(j_0 - j))$ with $x(f^{-1}(j_0 + 1 + j))$ where j takes the values $1, \ldots, j_0 - j_3$. The x' which results has domain $\mathrm{dom}(x') = \{i \in \mathrm{dom}(x) : i < i_3 \text{ or } i > P(i_3)\}$. We set $P' = P \setminus \{\{i, P(i)\} : i \in A\}$.

The only non trivial thing is to prove that P' satisfies GP4. Let $B = \{i \in \mathrm{su}(x') : i < i_3 \text{ and } P(i) > P(i_3)\}$. If for an equivalence class $\{k_1, k_2\}$ of P' we have $\{k_1, k_2\} \cap B = \emptyset$ then it is immediate that there exists some $k_3 \in \mathrm{dom}(x')$ between k_1 and k_2 with $k_3 \notin \mathrm{su}(x')$. So assume that B is not empty and let i_4 be its greatest element.

Case 2.1.1: There exists some $i_5 \in \mathrm{dom}(x')$ with $i_4 < i_5 < i_3$. If $i_5 \notin \mathrm{su}(x')$ then we immediately have what we want. If $i_5 \in \mathrm{su}(x')$ then $i_5 \notin B$ therefore $i_4 < P(i_5) < i_3$ and there exists some $k_3 \in \mathrm{dom}(x')$ between i_5 and $P(i_5)$ with $k_3 \notin \mathrm{su}(x')$.

Case 2.1.2: $i_4 \approx i_3$ in $\mathrm{dom}(x)$. Since $i_4 \notin A$, it follows that $f(i_0) - f(i_4) \neq f(P(i_4)) - f(i'_0)$ therefore it is not the case that $P(i_4) \approx P(i_3)$ in $\mathrm{dom}(x)$ so there exists $i_7 \in \mathrm{dom}(x')$ with $P(i_3) < i_7 < P(i_4)$ and the rest of the argument should be familiar to the reader by now.

Case 2.2: A is empty. x' is defined as the restriction of x to the set $\mathrm{dom}(x) \setminus \{i_0, i'_0\}$ and $P' = P$. Proving that P' satisfies GP4 is an easier version of the argument in case 2.1.
□

12. Corollary: If some $x \in \mathbb{GW}$ is not reduced and has a GP P then by a sequence of cancellations from x we get a reduced $x' \in \mathbb{GW}$ which has some GP P'.

13. Definition: Let $x \in \mathbb{GW}$ with a GP P. Let $A = \mathrm{dom}(x)$ and let $B \subset \mathbb{N}$ with $\mathrm{card}(A) = \mathrm{card}(B)$. Let $f = \mathrm{SI}(B, A)$ and $x' = \mathrm{tr}(x, A, B)$. Obviously $\mathrm{su}(x') = \{i \in B : f(i) \in \mathrm{su}(x)\}$. We define $\mathrm{tr}(P, A, B)$ to be the equivalence relation on $\mathrm{su}(x')$ which has the set of equivalence classes

$\{\{i_1, i_2\} : \{f(i_1), f(i_2)\} \in P\}$. Then it's obvious that $\mathrm{tr}(P, A, B)$ is a GP for x'.

14. Proposition: If some $x \in \mathbb{F}$ has a GP then $\mathfrak{r}(x)$ also has a GP.
Proof: Clearly for every $x_1 \in \mathbb{GW}$ with $A = \mathrm{dom}(x_1)$ and every $B \subset \mathbb{N}$ with $\mathrm{card}(A) = \mathrm{card}(B)$, x_1 is reduced iff $\mathrm{tr}(x_1, A, B)$ is reduced.

So, if $x \in \mathbb{F}$ has a GP, let $x' \in \mathbb{GW}$ be as given by corollary 12. Then $\mathfrak{r}(x) = \mathrm{tr}(x', \mathrm{dom}(x'), \mathrm{card}(\mathrm{dom}(x')))$ has a GP.
□

15. Definition: Let $x_1, x_2 \in \mathbb{GW}$. We define the *concatenation* of x_1 and x_2, in notation $x_1 \odot x_2$, as follows: for $i = 1, 2$ let $A_i = \mathrm{dom}(x_i)$ and $n_i = \mathrm{card}(A_i)$. $x_1 \odot x_2$ has domain $n_1 + n_2$ and for each j in the domain, $(x_1 \odot x_2)(j) = \mathrm{tr}(x_1, A_1, n_1)(j)$ if $j < n_2$, otherwise $(x_1 \odot x_2)(j) = \mathrm{tr}(x_2, A_2, n_2)(j - n_1)$.

It's easy to see that concatenation is associative.

16. Proposition: Let $x_1, x_2 \in \mathbb{GW}$ with GPs P_1 and P_2 respectively. Then the following hold:

1. $x_1 \odot x_2$ has a GP.
2. If $\mathrm{dom}(x_1) \neq \emptyset$ then for every $t \in \overline{X} \setminus \overline{Y}$, $t \odot x_1 \odot t^{-1}$ has a GP.
3. For every $t \in \overline{Y}$, $t \odot x_1$ and $x_1 \odot t$ have a GP.

Proof: Let $A_1 = \mathrm{dom}(x_1)$, $n_1 = \mathrm{card}(A_1)$, $x_1' = \mathrm{tr}(x_1, A_1, n_1)$ and $P_1' = \mathrm{tr}(P_1, A_1, n_1)$.

1. Let $A_2 = \mathrm{dom}(x_2)$, $n_2 = \mathrm{card}(A_2)$, $B_2 = \{i + n_1 : i \in n_2\}$, $x_2' = \mathrm{tr}(x_2, A_2, B_2)$ and $P_2' = \mathrm{tr}(P_2, A_2, B_2)$. Then $x_1 \odot x_2 = x_1' \cup x_2'$ and $P_1' \cup P_2'$ is a GP for $x_1 \odot x_2$.

2. Let $x' = t \odot x_1 \odot t^{-1}$. Then $\mathrm{dom}(x') = n_1 + 2$ and $x'(0) = t$, $x'(n_1 + 1) = t^{-1}$ and for i with $1 \leq i \leq n_1$, $x'(i) = x_1'(i - 1)$. Let $B = \{i + 1 : i \in n_1\}$ and $P' = \mathrm{tr}(P_1, A_1, B)$. Then $P' \cup \{0, n_1 + 1\}$ is a GP for x'.

3. Trivial.
□

17. Proposition: Let $x_1, x_2 \in \mathbb{F}$ with GPs P_1 and P_2 respectively. Then the following elements of $\mathbb{F}$ also have a GP:

1. $x_1 \cdot x_2$.
2. for every $t \in \overline{X} \setminus \overline{Y}$, $t \cdot x_1 \cdot t^{-1}$.
3. for every $t \in \overline{Y}$, $t \cdot x_1$ and $x_1 \cdot t$.

Proof: 1 and 3 are immediate from propositions 16, 14 and the definition of multiplication on $\mathbb{F}$.

For 2, if x_1 is the identity of $\mathbb{F}$, it is immediate; otherwise we have $t \cdot x_1 \cdot t^{-1} = \mathfrak{r}(\mathfrak{r}(t \odot x_1) \odot t^{-1}) = \mathfrak{r}(t \odot x_1 \odot t^{-1})$. The last equality follows from the proof of proposition 2.5.6 in [GRI]. Then we use again propositions 16 and 14 to get the result we want.
□

18. Definitions: A *formation sequence* is a function $f : n \to \mathbb{F}$ (where $n \in \mathbb{N}$) such that for every $i \in n$ at least one of the following holds:

1. $f(i)$ is the identity of $\mathbb{F}$.
2. There exist $i_1, i_2 \in n$ with $i_1 < i$ and $i_2 < i$ such that $f(i) = f(i_1) \cdot f(i_2)$.
3. There exist $i_1 \in n$ with $i_1 < i$ and $t \in \overline{X} \setminus \overline{Y}$ such that $f(i) = t \cdot f(i_1) \cdot t^{-1}$.
4. There exist $i_1 \in n$ with $i_1 < i$ and $t \in \overline{Y}$ such that $f(i) = t \cdot f(i_1)$ or $f(i) = f(i_1) \cdot t$.

An element x of $\mathbb{F}$ will be called *well-formed* if there exists some formation sequence f and an $i \in \text{dom}(f)$ such that $f(i) = x$.

19. Proposition: For every $x \in \mathbb{F}$, $x \in N$ iff x is well-formed.
Proof: To prove that if x is well-formed then $x \in N$ take some formation sequence f and an $i \in \text{dom}(f)$ such that $f(i) = x$ and use induction on i.

For the inverse, note first that the concatenation of two formation sequences is again a formation sequence which implies that the set of well-formed elements is closed under multiplication. If $f : n \to \mathbb{F}$ is a formation sequence then we can define $f' : n \to \mathbb{F}$ with $f'(i) = f(i)^{-1}$ for all $i \in n$. Clearly f' is also a formation sequence which shows that the set of well-formed elements is closed under inverses. Let x be well-formed and $x' \in \mathbb{F}$. To prove that $x' \cdot x \cdot x'^{-1}$ is well-formed, use induction on the length of x'.

So the set of well-formed elements is a normal subgroup of $\mathbb{F}$ which contains $\overline{Y}$.
□

Corollary: Every $x \in N$ has a GP.
Proof: It follows from propositions 17 and 19.
Corollary: Proposition 7 holds.

And this is a proof/solution of the exercise in [ROB] I can believe in! But it turns out that we can prove some other interesting results.

20. Definitions: A *cancellations-free formation sequence* (CFFS for short) is a function $f : n \to \mathbb{F}$ (where $n \in \mathbb{N}$) such that for every $i \in n$ at least one of the following holds:

1. $f(i)$ is the identity of $\mathbb{F}$.

2. There exist $i_1, i_2 \in n$ with $i_1 < i$ and $i_2 < i$ such that $f(i) = f(i_1) \cdot f(i_2) = f(i_1) \odot f(i_2)$.
3. There exist $i_1 \in n$ with $i_1 < i$ and $t \in \overline{X} \setminus \overline{Y}$ such that $f(i) = t \cdot f(i_1) \cdot t^{-1} = t \odot f(i_1) \odot t^{-1}$.
4. There exist $i_1 \in n$ with $i_1 < i$ and $t \in \overline{Y}$ such that $f(i) = t \cdot f(i_1) = t \odot f(i_1)$ or $f(i) = f(i_1) \cdot t = f(i_1) \odot t$.

An element x of $\mathbb{F}$ will be called *cancellations-free well-formed* (CFWF) if there exists some CFFS f and an $i \in \text{dom}(f)$ such that $f(i) = x$.

21. Proposition: If some $x \in \mathbb{F}$ has a GP then x is CFWF.
Proof: Assume that it holds for all $x' \in \mathbb{F}$ with $\text{len}(x') < \text{len}(x)$. If $\text{su}(x) = \emptyset$ then obviously x is CFWF.

Assume that $\text{su}(x) \neq \emptyset$ and let $i_0 = \min(\text{su}(x))$. Let P be a GP for x. Let $n = \text{len}(x)$.

Case 1: $i_0 = 0$ and $P(i_0) = n - 1$. Let $A = \{i \in n : 0 < i < n - 1\}$.

Let $x_1 = x|_A$ and $P_1 = P \setminus \{0, n-1\}$. Then $x_1 \in \mathbb{GW}$ and P_1 is a GP for x_1. Let $x_2 = \text{tr}(x_1, A, n-2)$ and $P_2 = \text{tr}(P_1, A, n-2)$. The sequence x_2 was obtained by taking successive elements from x and $x \in \mathbb{F}$ so no cancellations are possible in x_2 therefore $x_2 \in \mathbb{F}$. From the remark in ¶13, P_2 is a GP for x_2 so, from the inductive hypothesis, x_2 is CFWF so there exist $m \in \mathbb{N}$ and $f : m \to \mathbb{F}$ and $j \in m$ such that f is a CFFS and $f(j) = x_2$. Then $x = x(0) \cdot x_2 \cdot x(n-1) = x(0) \odot x_2 \odot x(n-1)$ so clearly there is also a CFFS for x.

Case 2: $i_0 = 0$ and $P(i_0) < n - 1$.

Let $A = \{i \in n : i \leq P(i_0)\}$ and $B = \{i \in n : P(i_0) < i\}$. Let $n_2 = \text{card}(B)$. Let $x_1 = x|_A$ and $x_2 = x|_B$. From GP2 it follows that if $\{i, j\}$ in an equivalence class of P then $\{i, j\} \subseteq A$ or $\{i, j\} \subseteq B$. Let $P_1 = P \cap A \times A$ and $P_2 = P \cap B \times B$. Then P_1 is a GP for x_1 and P_2 is a GP for x_2. Let $x_3 = \text{tr}(x_2, B, n_2)$ and $P_3 = \text{tr}(P_2, B, n_2)$. Then $x_3 \in \mathbb{F}$ and P_3 is a GP for x_3. From the inductive hypothesis, x_1 and x_3 are CFWF and $x = x_1 \cdot x_3 = x_1 \odot x_3$ therefore x is also CFWF.

Case 3: $i_0 > 0$.

Let $A = \{i \in n : i < i_0\}$ and $B = \{i \in n : i_0 \leq i\}$. The remaining steps are the same as in case 2.
□

Finally, we collect together all the previous results.

22. Proposition: For every $x \in \mathbb{F}$ the following are equivalent:

1. $x \in N$.
2. There exists a GP for x.
3. x is CFWF.
4. x is well-formed.

Proof: $1 \Rightarrow 2$: This is the corollary to proposition 19.
$2 \Rightarrow 3$: Proposition 21.
$3 \Rightarrow 4$: Immediate from the definitions.
$4 \Rightarrow 1$: Proposition 19.
□

23. Example: Let $X = \{s_1, s_2, s_3, s_4\}$ and $Y = \{s_1, s_2, s_3\}$. Let $x = \langle s_1, s_4^{-1}, s_2, s_4^{-1}, s_3, s_4, s_4 \rangle$. One formation sequence f for x has 8 elements and is
$f(0) = \mathbb{1}$
$f(1) = s_1 \cdot f(0) = \langle s_1 \rangle$
$f(2) = s_4 \cdot f(1) \cdot s_4^{-1} = \langle s_4, s_1, s_4^{-1} \rangle$
$f(3) = s_3 \cdot f(0) = \langle s_3 \rangle$
$f(4) = s_4^{-1} \cdot f(3) \cdot s_4 = \langle s_4^{-1}, s_3, s_4 \rangle$
$f(5) = s_2 \cdot f(4) = \langle s_2, s_4^{-1}, s_3, s_4 \rangle$
$f(6) = f(2) \cdot f(5) = \langle s_4, s_1, s_4^{-1}, s_2, s_4^{-1}, s_3, s_4 \rangle$
$f(7) = s_4^{-1} \cdot f(6) \cdot s_4 = x$

The product which gives $f(7)$ has cancellations. Proposition 22 tells us that there exists also a CFFS for x. The reader may find it interesting to come up with one.

3 The direct approach

This is another way to try and prove proposition 7. As I've said earlier, I couldn't manage to make it work in general but I'm including it because I'm curious whether any readers may find a way to make it work in general.

24. Definitions: For every $x \in \mathbb{F}$ and every $m \leq \text{len}(x)$, $\text{ini}(x, m)$ will mean the subsequence of x which has the first m elements and $\text{fin}(x, m)$ will mean the subsequence of x which has the final m elements. We have the identity that for $m_1, m_2 \in \mathbb{N}$ with $m_1 + m_2 = \text{len}(x)$,

$$x = \text{ini}(x, m_1) \cdot \text{fin}(x, m_2) = \text{ini}(x, m_1) \odot \text{fin}(x, m_2)$$

.

For all $x_1, x_2 \in \mathbb{F}$, $\text{nce}(x_1, x_2)$ will mean $\max\{m \in \mathbb{N} : m \leq \text{len}(x_1)$ and $m \leq \text{len}(x_2)$ and $\text{fin}(x_1, m) = \text{ini}(x_2, m)^{-1}\}$. "nce" stands for "number of

cancelled elements" and tells us how many cancellations will happen when we form the product $x_1 \cdot x_2$. More precisely, if for some x_1, x_2 we set $m_0 = \mathrm{nce}(x_1, x_2)$ and also $x_3 = \mathrm{ini}(x_1, \mathrm{len}(x_1) - m_0)$, $x_4 = \mathrm{fin}(x_1, m_0)$, $x_5 = \mathrm{ini}(x_2, m_0)$ and $x_6 = \mathrm{fin}(x_2, \mathrm{len}(x_2) - m_0)$ then
$x_1 \cdot x_2 = \mathfrak{r}(x_1 \odot x_2) = \mathfrak{r}(x_3 \odot x_4 \odot x_5 \odot x_6) = \mathfrak{r}(x_3 \odot x_4 \odot x_4^{-1} \odot x_6) = \mathfrak{r}(x_3 \odot x_6) = x_3 \odot x_6 = x_3 \cdot x_6$.

A useful fact is that $\mathrm{nce}(x_1, x_2) = \mathrm{nce}(x_2^{-1}, x_1^{-1})$.

A $x \in \mathbb{F}$ will be called *pure* if all the elements of x are in $\overline{Y}$.

25. Proposition: Let $x_1, x_2 \in \mathbb{F}$ be such that $\mathrm{nce}(x_1, x_2) = 0$ and x_2 pure. Then $x_1 \cdot x_2^{-1} \cdot x_1^{-1}$ has at least $\mathrm{len}(x_2)$ elements from $\overline{Y}$.
Proof: Assume that it holds for all $x_1', x_2' \in \mathbb{F}$ with $\mathrm{len}(x_1') + \mathrm{len}(x_2') < \mathrm{len}(x_1) + \mathrm{len}(x_2)$.

Obviously it holds if $\mathrm{len}(x_2) = 0$. Assume that $\mathrm{len}(x_2) > 0$.

Let $m_0 = \mathrm{nce}(x_1, x_2^{-1})$, $x_3 = \mathrm{ini}(x_1, \mathrm{len}(x_1) - m_0)$, $x_4 = \mathrm{fin}(x_1, m_0)$ and $x_5 = \mathrm{fin}(x_2^{-1}, \mathrm{len}(x_2) - m_0)$. Then $x_1 \cdot x_2^{-1} \cdot x_1^{-1} = x_3 \cdot x_4 \cdot x_4^{-1} \cdot x_5 \cdot x_1^{-1} = x_3 \cdot x_5 \cdot x_1^{-1}$.

Assume $\mathrm{len}(x_5) > 0$. $\mathrm{nce}(x_1, x_2) = 0 \Rightarrow \mathrm{nce}(x_2^{-1}, x_1^{-1}) = 0$ and $x_2^{-1} = x_4^{-1} \odot x_5$ therefore $x_5 \cdot x_1^{-1} = x_5 \odot x_1^{-1}$. Also, by the way x_3 and x_5 were defined, $x_3 \cdot x_5 = x_3 \odot x_5$. So

$$x_3 \cdot x_5 \cdot x_1^{-1} = x_3 \odot x_5 \odot x_1^{-1} = x_3 \odot x_5 \odot x_4^{-1} \odot x_3^{-1}$$

which has at least $\mathrm{len}(x_5) + \mathrm{len}(x_4^{-1})$ elements from $\overline{Y}$. $\mathrm{len}(x_5) + \mathrm{len}(x_4^{-1}) = \mathrm{len}(x_2^{-1}) = \mathrm{len}(x_2)$.

Assume now that $\mathrm{len}(x_5) = 0$. Then $x_2^{-1} = x_4^{-1}$ and $x_3 \cdot x_5 \cdot x_1^{-1} = x_3 \cdot x_1^{-1} = x_3 \cdot x_4^{-1} \cdot x_3^{-1}$. Then x_4 is pure , $\mathrm{nce}(x_3, x_4) = 0$ and $\mathrm{len}(x_3) + \mathrm{len}(x_4) = \mathrm{len}(x_1) < \mathrm{len}(x_1) + \mathrm{len}(x_2)$. Therefore, from the inductive hypothesis, $x_3 \cdot x_4^{-1} \cdot x_3^{-1}$ has at least $\mathrm{len}(x_4) = \mathrm{len}(x_2)$ elements from $\overline{Y}$.
□

26. Proposition: Let $x, y \in \mathbb{F}$ with y pure. Set $n = \mathrm{len}(y)$, $m = \mathrm{nce}(x, y)$ and $m' = \mathrm{nce}(\mathrm{fin}(y, n-m), x^{-1})$. Then $x \cdot y \cdot x^{-1}$ has at least $n - m - m' + |m - m'|$ elements from $\overline{Y}$. Furthermore, $n - m - m' + |m - m'| = 0$ iff $x \cdot y \cdot x^{-1} = \mathbb{1}$.
Proof: Case 1: $m + m' < n$ and $m \geq m'$.

Let $x_1 = \mathrm{ini}(x, \mathrm{len}(x) - m)$, $x_2 = \mathrm{ini}(\mathrm{fin}(x, m), m - m')$ and $x_3 = \mathrm{fin}(x, m')$. So we have $x = x_1 \odot x_2 \odot x_3$. Let $y_1 = \mathrm{ini}(y, m)$, $y_2 = \mathrm{ini}(\mathrm{fin}(y, n - m), n - m - m')$ and $y_3 = \mathrm{fin}(y, m')$. Then

$$x \cdot y \cdot x^{-1} = x_1 \cdot (x_2 \cdot x_3 \cdot y_1) \cdot y_2 \cdot (y_3 \cdot x_3^{-1}) \cdot x_2^{-1} \cdot x_1^{-1} = x_1 \cdot y_2 \cdot x_2^{-1} \cdot x_1^{-1}$$

By the definitions of x_1, x_2, y_2 it follows that $x_1 \cdot y_2 = x_1 \odot y_2$ and $y_2 \cdot x_2^{-1} = y_2 \odot x_2^{-1}$. So $x_1 \cdot y_2 \cdot x_2^{-1} \cdot x_1^{-1}$ has at least $\text{len}(y_2) + \text{len}(x_2^{-1})$ elements from $\overline{Y}$ so $n - m - m' + |m - m'|$ elements.

Case 2: $m + m' = n$ and $m \geq m'$.

We define x_1, x_2, x_3, y_1, y_2, y_3 as in case 1. Now $\text{len}(y_2) = 0$ so $y_2 = \imath$ therefore

$$x \cdot y \cdot x^{-1} = x_1 \cdot x_2^{-1} \cdot x_1^{-1}$$

$\text{nce}(x_1, x_2) = 0$ because they are adjacent subsequences of x so from proposition 25 it follows that $x_1 \cdot x_2^{-1} \cdot x_1^{-1}$ has at least $\text{len}(x_2)$ elements from $\overline{Y}$ which makes it $m - m' = |m - m'|$ elements.

Case 3: $m + m' < n$ and $m < m'$.

Let $x_1 = \text{ini}(x, \text{len}(x) - m')$, $x_2 = \text{ini}(\text{fin}(x, m'), m' - m)$ and $x_3 = \text{fin}(x, m)$. Again we have $x = x_1 \odot x_2 \odot x_3$. Let $y_1 = \text{ini}(y, m)$, $y_2 = \text{ini}(\text{fin}(y, n - m), n - m - m')$ and $y_3 = \text{fin}(y, m')$. Then

$$x \cdot y \cdot x^{-1} = x_1 \cdot x_2 \cdot (x_3 \cdot y_1) \cdot y_2 \cdot (y_3 \cdot x_3^{-1} \cdot x_2^{-1}) \cdot x_1^{-1} = x_1 \cdot x_2 \cdot y_2 \cdot x_1^{-1}$$

As with case 1 we have that $x_1 \cdot x_2 \cdot y_2 \cdot x_1^{-1} = x_1 \odot x_2 \odot y_2 \odot x_1^{-1}$ which has at least $\text{len}(x_2) + \text{len}(y_2) = m' - m + n - m - m' = n - 2 \cdot m$ elements from $\overline{Y}$.

Case 4: $m + m' = n$ and $m < m'$.

The overall pattern should be clear by now so I'll leave that for the reader. □

The next step in this approach was to try and prove a proposition analogous to 26 but more complicated. After experimenting with various things, the most promising seemed to be

Let $x_1, x_2, x_3, y_1, y_2 \in \mathbb{F}$ with y_1, y_2 pure. Then

$$x_1 \cdot x_2 \cdot y_1 \cdot x_2^{-1} \cdot x_3 \cdot y_2 \cdot x_3^{-1} \cdot x_1^{-1}$$

is either the identity or has at least one element from $\overline{Y}$.

The approach of the proof was supposed to be analogous to proposition 26, namely break x_1, x_2, x_3, y_1, y_2 into subsequences which cancel out with each other when you form the product above and then distinguish cases based on the relative lengths of these subsequences. I could make some of these cases work but with others I got stuck and, interestingly, not the ones which seemed most complicated on first look. I started considering different approaches and eventually came up with the one in the previous section.

4 Chuck Norris facts

To the best of my knowledge, there are no Chuck Norris facts associated with this work.

♠♠♠♠♠♠♠♠♠♠♠

Spiros Bousbouras, September 2023.

You can contact me at

$(@^{-1} \cdot u^{-1} \cdot o^{-1} \cdot b^{-1} \cdot i^{-1} \cdot p^{-1} \cdot s^{-1})^{-1} \cdot ((c \cdot o \cdot m)^{-1} \cdot .^{-1} (g \cdot m \cdot a \cdot i \cdot l)^{-1})^{-1}$