Selected Solutions from Aluffi's Algebra

Ian Beard

Last updated November 2 2024

Exercise II.8.7

Let $\langle A \mid R\rangle$ and $\langle A' \mid R'\rangle$ be presentations for groups G and G' respectively. Assume that A and A' are disjoint.

Claim 1. *The group $G*G'$ presented by $\langle A\cup A' \mid R\cup R'\rangle$ satisfies the universal property for the coproduct of G and G' in **Grp**.*

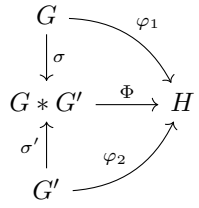
Proof. To show this, we first acquire some natural homomorphisms from $G \to G*G'$ and $G' \to G*G'$. For the homomorphism from $G \to G*G'$, consider the set map $\iota^\star : A \to F(A\cup A') \Big/ \langle\langle R\cup R'\rangle\rangle \cong G*G'$ defined by $\iota^\star(a) = \overline{a}\langle\langle R\cup R'\rangle\rangle$ where $\overline{a}$ is image of a in the free group $F(A\cup A')$. Then by the universal property of free groups there exists a unique group homomorphism φ making the following diagram commute.

$$\begin{array}{ccc} A & \xrightarrow{\iota^\star} & G*G' \\ \downarrow{\scriptstyle \iota} & \nearrow{\scriptstyle \varphi} & \\ F(A) & & \end{array}$$

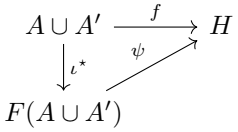
Now I claim that $\langle\langle R\rangle\rangle$ is contained in $\ker\varphi$. Let $r \in \langle\langle R\rangle\rangle$. Then $r = (w_1 r_1 w_1^{-1})\cdots(w_n r_n w_n^{-1})$ for some $w_i \in F(A)$ and $r_i \in R$. To show that $\varphi(r) = 1$, it suffices to show that $\varphi(r_i) = 1$ for any $r_i \in R$, since φ is a homomorphism. Now $r_i = \iota(a_1)\ldots\iota(a_n)$ for some $a_i \in A$. Then $\varphi(r) = \varphi(\iota(a_1))\ldots\varphi(\iota(a_n)) = \iota^\star(a_1)\ldots\iota^\star(a_n) = \overline{a_1}\ldots\overline{a_n}\langle\langle R\cup R'\rangle\rangle = \langle\langle R\cup R'\rangle\rangle$ since $\overline{a_1}\ldots\overline{a_n} \in \langle\langle R\rangle\rangle \subseteq \langle\langle R\cup R'\rangle\rangle$. Thus $R \subseteq \ker\varphi$, which is what we needed to conclude that $\langle\langle R\rangle\rangle \subseteq \ker\varphi$. By the universal property of quotients, there exists a unique homomorphism $\sigma : F(A) \Big/ \langle\langle R\rangle\rangle \cong G \to G*G'$ such that the following diagram commutes, where π is the canonical quotient map.

$$\begin{array}{ccc} A & \xrightarrow{\iota^\star} & G*G' \\ \downarrow{\scriptstyle \iota} & \nearrow{\scriptstyle \varphi} & \uparrow{\scriptstyle \sigma} \\ F(A) & \xrightarrow{\pi} & G \end{array}$$

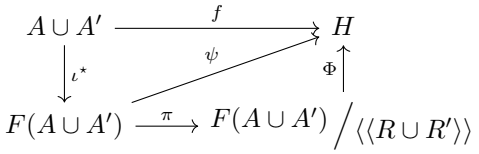
This homomorphism $\sigma : G \to G * G'$ was the desired homomorphism, and by mirroring this process we can get a similar homomorphism $\sigma' : G' \to G * G'$. Now, we claim that $(G * G', \sigma, \sigma')$ satisfies the universal property for coproducts in the category **Grp**. That is, for any group homomorphisms $\varphi_1 : G \to H$ and $\varphi_2 : G' \to H$ there exists a unique group homomorphism Φ such that the following diagram commutes.



Suppose we are given such homomorphisms φ_1 and φ_2. From here on, let $\iota : A \to F(A)$ and $\iota' : A' \to F(A')$ be the canonical injections, and $\pi : F(A) \to F(A)\Big/\langle\langle R \rangle\rangle \cong G$ and $\pi' : F(A') \to F(A')\Big/\langle\langle R' \rangle\rangle \cong G'$ be the canonical quotient maps. Now, define a set map $f : A \cup A' \to H$ by $f(a) = \varphi_1 \circ \pi \circ \iota(a)$ if $a \in A$, and $f(a') = \varphi_2 \circ \pi' \circ \iota'(a')$ if $a' \in A'$. This is a well-defined map since $A \cap A' = \varnothing$. Then by the universal property of free groups there exists a unique homomorphism ψ such that the following diagram commutes.



where $\iota^\star$ is the canonical injection. By similar reasoning as in the previous portion, it can be shown that $R \cup R' \subseteq \ker\psi$, and moreover that $\langle\langle R \cup R' \rangle\rangle \subseteq \ker\psi$. Thus, there exists a unique homomorphism Φ such that the following diagram commutes.



Now, I claim that $\Phi : F(A \cup A')\Big/\langle\langle R \cup R' \rangle\rangle \cong G * G' \to H$ is the unique homomorphism making our desired diagram commute. I first show that $\Phi \circ \sigma =$

φ_1. Let $\overline{a_1} \dots \overline{a_n}\langle\langle R \rangle\rangle$ be an element of G, where $a_i \in A$ and $\overline{a_i} = \iota(a_i)$. Then

$$\begin{aligned}
\Phi \circ \sigma(\overline{a_1} \dots \overline{a_n}\langle\langle R \rangle\rangle) &= \Phi \circ \sigma(\overline{a_1}\langle\langle R \rangle\rangle) \dots \Phi \circ \sigma(\overline{a_n}\langle\langle R \rangle\rangle) \\
&= \Phi \circ (\overline{a_1}\langle\langle R \cup R' \rangle\rangle) \dots \Phi \circ (\overline{a_n}\langle\langle R \cup R' \rangle\rangle) \\
&= \Phi \circ (\pi \circ \iota^\star(a_1)) \dots \Phi \circ (\pi \circ \iota^\star(a_n)) \\
&= \varphi_1 \circ \pi \circ \iota(a_1) \dots \varphi_1 \circ \pi \circ \iota(a_n)
\end{aligned}$$

By how f was defined and the fact that $\Phi \circ \pi \circ \iota^\star = f$. Then we have:

$$\begin{aligned}
\Phi \circ \sigma(\overline{a_1} \dots \overline{a_n}\langle\langle R \rangle\rangle) &= \varphi_1 \circ \pi \circ \iota(a_1) \dots \varphi_1 \circ \pi \circ \iota(a_n) \\
&= \varphi_1(\overline{a_1}\langle\langle R \rangle\rangle) \dots \varphi_1(\overline{a_n}\langle\langle R \rangle\rangle) \\
&= \varphi_1(\overline{a_1} \dots \overline{a_n}\langle\langle R \rangle\rangle)
\end{aligned}$$

Showing that $\Phi \circ \sigma = \varphi_1$. A mirror argument shows that $\Phi \circ \sigma' = \varphi_2$, so that Φ indeed makes the desired diagram commute. All that is left to show is that Φ is the unique homomorphism which does so.

For Φ to make the diagram commute, we must necessarily have that $\Phi(\overline{a}\langle\langle R \cup R' \rangle\rangle) = \varphi_1(\overline{a}\langle\langle R \rangle\rangle)$ for all letters $a \in A$, and similarly that $\Phi(\overline{a'}\langle\langle R \cup R' \rangle\rangle) = \varphi_2(\overline{a'}\langle\langle R' \rangle\rangle)$ for all letters $a' \in A'$. Since this information completely determines the homomorphism Φ, we must have that Φ is the unique homomorphism making the diagram commute. $\square$

Exercise II.8.17

Assume that G is a finite abelian group, and p is a prime divisor of $|G|$.

Claim 1. *There exists an element of order p in G.*

Proof. First, let $g \in G$ be an arbitrary non-trivial element and consider the subgroup it generates $\langle g \rangle$. Since $\langle g \rangle$ is non-trivial there must exist a prime integer q such that $q \mid |\langle g \rangle|$. Thus, there exists an integer m such that $|\langle g \rangle| = mq$. Now, consider the element $g^m \in \langle g \rangle$. We know that

$$\begin{aligned} |g^m| &= \frac{\operatorname{lcm}(|g|, m)}{m} \\ &= \frac{\operatorname{lcm}(mq, m)}{m} \\ &= \frac{mq}{m} = q \end{aligned}$$

Thus, g^m is an element of order q in G. If $q = p$, we are finished. Otherwise, consider the group $G/\langle g^m \rangle$ and iterate the process, finding another element of prime order. If we repeat this process enough times, without having found an element of order p, we will arrive at the quotient group G/H such that $|G/H| = p^k$ for some positive integer k and $p \nmid |H|$. G/H will certainly have an element of order p, call it $\tilde{g}H$. Now $|\tilde{g}H| = p$ implies that p is the least positive integer such that $\tilde{g}^p \in H$. Now, since $\gcd(p, |H|) = 1$, the map $f : H \to H$ sending $h \mapsto h^p$ is a surjection. Thus, there exists $\tilde{h} \in H$ such that $\tilde{h}^p = (\tilde{g}^p)^{-1}$. I claim that the element $\tilde{g}\tilde{h} \in G$ is the desired element of order p. First, notice that $(\tilde{g}\tilde{h})^p = \tilde{g}^p\tilde{h}^p = \tilde{g}^p(\tilde{g}^p)^{-1} = e$, so that $|\tilde{g}\tilde{h}|$ must be 1 or p. If $|\tilde{g}\tilde{h}| = 1$ then $\tilde{g} = \tilde{h}^{-1} \in H$, a contradiction. Therefore, $\tilde{g}\tilde{h}$ is an element of order p. □

Exercise II.8.20

Let G be a finite abelian group and d be a positive divisor of $|G|$.

Claim 1. *There exists a subgroup of G of order d.*

Proof. To prove this, we first prove the weaker statement that if a prime power p^k divides $|G|$ then there exists a subgroup of order p^k. We show this by inducting on the power k. For the base case $k = 1$, we refer to the previous exercise which proved that there exists an element, and thus a subgroup, of order p. Now, assume the hypothesis is true for k, and consider a finite abelian group such that $p^{k+1} \mid G$. First, find an element $g \in G$ of order p and consider the quotient $G/\langle g\rangle$ which is such that $p^k \mid |G/\langle g\rangle|$. By the induction hypothesis, there exists a subgroup $K \leq G/\langle g\rangle$ such that $|K| = p^k$. Consider the canonical quotient map $\pi : G \to G/\langle g\rangle$. Define a new map $\varphi : \pi^{-1}(K) \to K$ by $\varphi(a) \mapsto a\langle g\rangle$. If $a \in \pi^{-1}(K)$ then $\pi(a) = a\langle g\rangle \in K$ so that φ is well-defined. Since $\varphi(ab) = ab\langle g\rangle = a\langle g\rangle b\langle g\rangle = \varphi(a)\varphi(b)$ it's clear that φ is a group homomorphism. Since π is surjective and $K \leq G/\langle g\rangle$ we also see that φ is surjective. Moreover, the kernel of φ are the elements $a \in \pi^{-1}(K)$ such that $a\langle g\rangle = \langle g\rangle$. In other words, $\ker\varphi = \pi^{-1}(K) \cap \langle g\rangle = \langle g\rangle$ since $\langle g\rangle \subseteq \pi^{-1}(K)$. Thus, we have that $\pi^{-1}(K)/\langle g\rangle \cong K$. Moreover, we get the equality $|\pi^{-1}(K)| = |K| \cdot |\langle g\rangle| = p^k \cdot p = p^{k+1}$. Therefore, $\pi^{-1}(K)$ is the desired subgroup of order p^k.

Now, let us return to the case of a general divisor $d \mid G$. We can obtain a prime factorization $d = p_1^{k_1} \dots p_n^{k_n}$. For each $p_i^{k_i}$ let us find a subgroup K_i such that $|K_i| = p_i^{k_i}$. Since G is abelian, we can form the product group $K = K_1 \dots K_n = \{k_1 \cdots k_n \mid k_i \in K_i\}$. Since the orders of groups K_i are pairwise coprime, we get that $|K| = |K_1| \cdots |K_n| = p_1^{k_1} \cdots p_n^{k_n} = d$. Therefore, K is the desired subgroup of order d. □