

Algebra: Chapter 0 Exercises

Chapter 2, Section 8

David Melendez

August 11, 2017

Problem 8.1. If a group H may be realized as a subgroup of two groups G_1 and G_2 , and

$$\frac{G_1}{H} \cong \frac{G_2}{H},$$

does it follow that $G_1 \cong G_2$? Give a proof or counterexample

Solution. No. As a counterexample, take $G_1 = D_6$, $G_2 = C_6$, and $H = C_3$. In this case, we have $D_6/C_3 \cong C_2 \cong C_6/C_3$, but $D_6 \not\cong C_3$. ■

Problem 8.2. Suppose G is a group, and $H \subseteq G$ is a subgroup of index 2. Prove that H is normal in G .

Solution. Consider the function $\varphi : G \rightarrow C_2$ defined by

$$\varphi(g) = \begin{cases} 0 & g \in H \\ 1 & g \notin H \end{cases}$$

To check that this is a homomorphism, suppose $g_1, g_2 \notin H$. In particular, $g_2^{-1} \notin H$, so

$$g_1H = g_2^{-1}H,$$

since there are only two left cosets of H in G , so

$$g_1g_2 \in H$$

and hence

$$\begin{aligned} \varphi(g_1g_2) &= 0 \\ &= 1 + 1 \\ &= \varphi(g_1) + \varphi(g_2). \end{aligned}$$

Clearly $\ker \varphi = H$, so H is normal in G . ■

Problem 8.7. Let $\langle A|\mathcal{R} \rangle$ resp. $\langle A'|\mathcal{R}' \rangle$ be presentations for two groups G resp. G' ; we may assume that A and A' are disjoint. Prove that the groups $G * G'$ presented by

$$\langle A \cup A' | \mathcal{R} \cup \mathcal{R}' \rangle$$

satisfies the universal property for the coproduct of G and G' in **Grp**.

Solution. Let G, G' and $A, A', \mathcal{R}, \mathcal{R}'$ be as described above, let R resp. R' resp. \hat{R} be the normal closures of \mathcal{R} resp. \mathcal{R}' $\mathcal{R} \cup \mathcal{R}'$, and let H be any group. Consider the diagram below, in which we use the universal properties of free groups and quotient groups to construct two morphisms $\tau : G \rightarrow G * G'$ and $\tau' : G' \rightarrow G * G'$:

$$\begin{array}{ccccc}
 & & H & & \\
 & \nearrow \varphi & \uparrow \hat{\varphi} & \nwarrow \varphi' & \\
 \frac{F(A)}{R} & \xrightarrow{\tau} & \frac{F(A \cup A')}{\hat{R}} & \xleftarrow{\tau'} & \frac{F(A')}{R'} \\
 \uparrow \pi & \nearrow q & \uparrow \hat{\pi} & \nwarrow q' & \uparrow \pi' \\
 F(A) & \xrightarrow{p} & F(A \cup A') & \xleftarrow{p'} & F(A') \\
 \uparrow j & \nearrow u & \uparrow \hat{j} & \nwarrow u' & \uparrow j' \\
 A & \xrightarrow{\iota} & A \cup A' & \xleftarrow{\iota'} & A'
 \end{array}$$

Here, ι and ι' are canonical inclusions (since A and A' are disjoint), j, \hat{j}, j' are the canonical inclusions into the free groups, u resp. u' are defined by $\hat{j}\iota$ resp. $\hat{j}\iota'$, and p and p' are obtained by applying the universal property of free groups.

The morphisms $\pi, \hat{\pi}$, and π' are the canonical projections, q resp. q' are defined by $\hat{\pi}p$ resp. $\hat{\pi}p'$, and τ and τ' are obtained by invoking the universal property of quotient groups.

Finally, φ, φ' are any morphisms, and we propose that there exists a unique morphism $\hat{\varphi}$ such that $\hat{\varphi}\tau = \varphi$ and $\hat{\varphi}\tau' = \varphi'$. For this, we simply must prove that if we define $\hat{\varphi}$ by those two relations, then $\hat{\varphi}$ is well defined.

Hence, suppose $\tau(w_1R) = \tau(w_2R)$. We then have

$$\tau(\pi(w_1)) = \tau(\pi(w_2)),$$

and hence

$$q(w_1w_2^{-1}) = 0.$$

Note that

$$\begin{aligned}
 \ker q &= \ker(\hat{\pi}p) \\
 &= \ker(p) \cup p^{-1}(\ker \hat{\pi}) \\
 &= p^{-1}(\ker \hat{\pi}) \\
 &= p^{-1}(\hat{R}) \\
 &= R.
 \end{aligned}$$

This tells us that $w_1w_2^{-1} \in R$, and so $w_1R = w_2R$; hence τ is injective. The same reasoning applies to τ' . Since $F(A \cup A')/\hat{R}$ is generated by the images of τ and τ' , this $\hat{\varphi}$ is well-defined, and hence unique. ■

Problem 8.12. Prove 'by hand' (that is, by using Proposition 6.2), that if H, K are subgroups of G , then HK is a subgroup of G if H is normal.

Solution. Let h_1, h_2 and k_1, k_2 be in H and K , respectively. We then have

$$\begin{aligned}(h_1 k_1)(h_2 k_2)^{-1} &= h_1 k_1 k_2^{-1} h_2^{-1} \\ &= k_1 (k_1^{-1} h_1 k_1) (k_2^{-1} h_2^{-1} k_2) k_2^{-1} \\ &= k_1 h' h'' k_1^{-1} \\ &\in H.\end{aligned}$$

Hence HK is a group by Proposition 6.2. ■

Problem 8.13. Let G be a finite commutative group, and assume $|G|$ is odd. Prove that every element of G is a square.

Solution. Let $g \in G$. Since $|G|$ is odd, $|g|$ is also odd (by Lagrange's Theorem), so $|g| + 1$ is even. We then have

$$\begin{aligned}\left(g^{\frac{|g|+1}{2}}\right)^2 &= g^{|g|+1} \\ &= g\end{aligned}$$

Hence g is a square. ■

Problem 8.14. Generalize the result of Exercise 8.13: if G is a group of order n , and k is an integer relatively prime to n , then the function $G \rightarrow G$, $g \mapsto g^k$ is surjective.

Proof. Suppose $g \in G$. If $\gcd(k, n) = 1$, then by Lagrange's Theorem, we have $\gcd(|g|, k) = 1$ as well. Hence there exist integers a and b such that $a|g| + bk = 1$. Let a, b be integers that satisfy this property. We then have:

$$\begin{aligned}g &= g^{a|g|+bk} \\ &= g^{a|g|} g^{bk} \\ &= g^{bk} \\ &= (g^b)^k\end{aligned}$$

Hence every $g \in G$ is in the image of the map mentioned above. □

Problem 8.15. Let a, n be positive integers. Prove that n divides $\phi(a^n - 1)$, where ϕ is Euler's ϕ -function.

Solution. Let $m = a^n - 1$, and consider the group $G = (\mathbb{Z}/m\mathbb{Z})^*$. If $a = 1$ then the question is nonsense, and if $n = 1$ then clearly $1 | \phi(a - 1)$. Hence, assume that $m > 1$ and $n > 1$. We know that $a \in G$ because $a^n - 1 > a$ and $\gcd(a, a^n - 1) = 1$. We also know that

$$a^n \equiv 1 \pmod{m}.$$

Since $x < n$ implies

$$1 < a \leq a^x < a^n - 1,$$

it then follows that $|a| = n$, and hence $n \mid |G| = \phi(a^n - 1)$. ■

Problem 8.16. Generalize Fermat's Little Theorem to congruences modulo arbitrary integers.

Solution.

Euler's Theorem. Let a, b be positive integers. Then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof. We have $[a^{\phi(n)}]_n = [1]_n$ in $(\mathbb{Z}/n\mathbb{Z})^*$. □

Problem 8.17. Assume G is a finite abelian group, and let p be a prime divisor of $|G|$. Prove that there exists an element in G of order p .

Solution. Let $G_0 = G$. We will soon define each G_k to be a quotient G_{k-1}/H , where H is a subgroup of prime order. We will proceed by (strong) induction on this subscript k , proving that, for $0 \leq k < \Omega(|G|)$:

1. If $\Omega(n)$ is the number of prime divisors of n including multiplicity, then

$$\Omega(|G_k|) = \Omega(|G|) - k.$$

2. There exists an element of $|G_k|$ of prime order.

3. If $g \in G_k$, has prime order p , then there exists an element of G of order p .

Proof.

Base case ($n=0$): Let $G_0 = G$.

1. $\Omega(|G_0|) = \Omega(|G|) = \Omega(|G|) - 0$

2. Let $g_0 \in G_0$, and for some prime divisor q_0 of $|g_0|$, let $h_0 = g_0^{\frac{|g_0|}{q_0}}$. We then have $|h_0| = q_0$, hence (2) holds.

3. Trivial.

Induction ($n = k + 1$): Suppose (1), (2), and (3) hold for $n \leq k$. Let $H_k = \langle h_k \rangle$ (which is normal because G is abelian), and define $G_{k+1} = G_k/H_k$.

1. We have:

$$\begin{aligned} \Omega(|G_{k+1}|) &= \Omega\left(\left|\frac{G_k}{H}\right|\right) \\ &= \Omega\left(\frac{|G_k|}{|H|}\right) \\ &= \Omega\left(\frac{|G_k|}{q}\right) \\ &= \Omega(|G_k|) - 1 \\ &= \Omega(G) - k - 1 \end{aligned}$$

as desired.

2. Same as the base case - let q_{k+1} be a prime divisor of $|G_{k+1}|$, let $g_{k+1} \in G_{k+1}$, and define $h_{k+1} := g_{k+1}^{\frac{|g_{k+1}|}{q_{k+1}}}$. Then $|h_{k+1}| = q_{k+1}$.
3. Suppose $gH_k \in G_{k+1}$ has order p , where p is a prime divisor of $|G_{k+1}|$. It then follows that $(gH_k)^p = e$, and so $g^p = h_k^m$ for some integer m . Since $e = (h^k)^x = g^{px}$ for some $x = |h^k|$, we then have $|g^x| = p$ in G_k . By our inductive hypothesis, then, we have an element of G of order p , as desired.

The set $\{q_0, \dots, q_n\}$ where $n = \Omega(G) - 1$ is the set of all prime divisors of $|G|$, since at each step of the process we have removed a prime divisor before choosing a new one.. At the end of this process, we have proven that G contains an element of order q_n for each n , and hence an element of order p for each prime divisor p of $|G|$. \square

Solution. [Alternative (better) proof]

Let p be any prime divisor of $|G|$. We will proceed by strong induction on $|G|$.

Base Case ($|G| = p$): Since $|G|$ is of prime order, it is cyclic, and so any non-identity element will be a generator, i.e. of order p .

Induction ($|G| = n$): Suppose the statement holds for every group of order $p \leq k < n$. Take some $g \in G$, and consider the group $\langle g \rangle$. If we take some prime divisor q of $|g|$, then $h := g^{\frac{|g|}{q}}$ has order q . If $q = p$, then we're done. Otherwise, let $H = \langle h \rangle$, and consider the group G/H .

We know that $|\frac{G}{H}| = \frac{|G|}{q} < |G|$. Moreover, p divides $|H|$, so by our inductive hypothesis, there exists a $gH \in G/H$ of order p . The same argument from part 3 of the inductive step of the other proof of this exercise applies here, giving us an element of G of order p , as desired. \blacksquare

Problem 8.18. Let G be an abelian group of order $2n$, where n is odd. Prove that G has exactly one element of order 2.

Solution. Let g, h be distinct elements of G . If g and h both have order 2, then the subgroup generated by g and h equals $\{e_G, g, h, gh\}$, which has order 4. But 4 is not a divisor of $|G| = 2n$ for n odd (otherwise n would be even), so g and h do not both have order 2.

This does not necessarily hold if G is not commutative. A counterexample is the dihedral group D_6 , where $f \neq rfr^{-1}$ both have order 2. \blacksquare

Problem 8.19. Let G be a finite group, and let d be a proper divisor of $|G|$. Is it necessarily true that there exists an element of G of order d ?

Solution. No. The group S_4 has no elements of order 8, or more generally, of order greater than 4. \blacksquare

Problem 8.20. Assume G is a finite abelian group, and let d be a proper divisor of $|G|$. Prove that there exists a subgroup $H \leq G$ of order d .

Solution. We will proceed by strong induction on the order of G .

Base Case ($|G| = 1$): Trivial.

Induction ($|G| = n$): Suppose every group of order $1 \leq k < n$ has a subgroup of order d for every integer $d \mid k$. Let p be a prime factor of d , and let $P = \langle p \rangle$. The group G/P is then of order $\frac{d}{p}x$ for some integer x . By our inductive hypothesis, there is a subgroup H of G/P with order $\frac{d}{p}$. If we define $\pi : G \rightarrow G/P$ to be the quotient map and let $K = \pi^{-1}(H)$, then $H = K/P$. It then follows that

$$\left| \frac{K}{P} \right| = \frac{d}{p}.$$

Hence

$$|K| = d.$$

as desired. ■

Problem 8.21. Let H, K be subgroups of a group G . Construct a bijection between the set of cosets hK with $h \in H$ and the set of left cosets of $H \cap K$ in H . If H and K are finite, prove that

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

Solution. Let H' be the set of cosets hK with $h \in H$, and consider the function

$$\begin{aligned} \varphi : H' &\rightarrow \frac{H}{H \cap K} \\ hK &\mapsto h(H \cap K). \end{aligned}$$

This function is well-defined:

$$\begin{aligned} h_1K = h_2K &\implies h_1h_2^{-1} \in K \\ &\implies h_1h_2^{-1} \in H \cap K \\ &\implies h_1(H \cap K) = h_2(H \cap K) \end{aligned}$$

(as $h_1h_2^{-1} \in H$ by closure).

This function is injective:

$$\begin{aligned} \varphi(h_1) = \varphi(h_2) &\implies h_1(H \cap K) = h_2(H \cap K) \\ &\implies h_1h_2^{-1} \in H \cap K \\ &\implies h_1h_2^{-1} \in K \\ &\implies h_1K = h_2K \end{aligned}$$

This function is surjective:

$$h(H \cap K) = \varphi(hK)$$

Hence φ is a bijection, and $|H'| = \left| \frac{H}{H \cap K} \right|$.
Next, define a function

$$\begin{aligned}\psi : H' &\rightarrow \frac{HK}{K} \\ hK &\mapsto (he_K)K \\ &= hK\end{aligned}$$

This function is quite clearly well-defined and injective. To prove that it's surjective, note that

$$\begin{aligned}(hk)K &= (he_K K)(e_H kK) \\ &= (hK)(kK) \\ &= hK \\ &= \psi(hK)\end{aligned}$$

Hence $|H'| \cong \frac{HK}{K}$. We then have,

$$\left| \frac{HK}{K} \right| = |H'| = \left| \frac{H}{H \cap K} \right|,$$

and so, by Langrange's theorem,

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

■

Problem 8.22. Let $\varphi : G \rightarrow G'$ be a group homomorphism, and let N be the smallest normal subgroup containing $\text{im } \varphi$. Prove that G'/N satisfies the universal property of coker φ in **Grp**.

Solution. Let K be a group, and let $\alpha : G' \rightarrow K$ be a homomorphism satisfying

$$\alpha \circ \varphi = 0,$$

or equivalently,

$$\text{im } \varphi \subseteq \ker \alpha.$$

Let $\pi : G' \rightarrow G'/N$ be the canonical projection. Since $\text{im } \varphi \subseteq N = \ker \pi$, $(G'/N, \pi)$ is an object in the relevant category.

Now, consider a morphism $\bar{\alpha} : G'/N \rightarrow K$ with the property

$$\bar{\alpha} \circ \pi = \alpha.$$

We then must have, for all $h_1, h_2 \in G'$,

$$h_1N = h_2N \implies \alpha(h_1) = \alpha(h_2)$$

in order for the morphism to be well defined. Suppose then, that $h_1N = h_2N$, or equivalently, that $h_1h_2^{-1} \in N$. Then there exist $g_i \in G'$ and $k_i \in \text{im } \varphi$ such that

$$h_1h_2^{-1} = \prod_{i=1}^n g_ik_ig_i^{-1}.$$

With this,

$$\begin{aligned} \alpha(h_1h_2^{-1}) &= \alpha\left(\prod_{i=1}^n g_ik_ig_i^{-1}\right) \\ &= \prod_{i=1}^n \alpha(g_i)\alpha(k_i)\alpha(g_i^{-1}) \\ &= \prod_{i=1}^n \alpha(g_i)\alpha(g_i^{-1}) \\ &= e_K \end{aligned}$$

and so

$$\alpha(h_1) = \alpha(h_2),$$

as desired. Since $\bar{\alpha}$ defined by the required relation is well-defined on $\text{im } \pi = G/N$, we are done. ■