Artin, Algebra, Chapter 2 Exercises

written by Dr. Heraklinos on Functor Network
original link: https://functor.network/user/842/entry/312

Problem 1.1. Let S be a set. Prove that the law of composition defined by $ab = a$ for all a and b in S is associative. For which sets does this law have an identity?

Solution. Given $a, b, c \in S$, one has

$$(ab)c = ac = a = ab = a(bc),$$

so this law of composition on S is associative. Next, I claim that this law has an identity element if and only if S is a singleton set. Indeed, if $S = \{s\}$, then $ss = s$, so s is the identity element. Conversely, suppose S contain an identity element e. Then, for any $a \in S$, one has $ae = a = ea$. But the law of composition implies that $ea = e$, hence $a = e$ and $S = \{e\}$.

Problem 1.3. Let $\mathbb{N}$ denote the set $\{1, 2, 3\}$ of natural numbers, and let $s : \mathbb{N} \to \mathbb{N}$ be the *shift* map defined by $s(n) = n + 1$. Prove that s has no right inverse, but that it has infinitely many left inverses.

Solution. Suppose, for the sake of contradiction, that there exists a right inverse $g : \mathbb{N} \to \mathbb{N}$ for s. Then $(s \circ g)(n) = n$ for every $n \in \mathbb{N}$. In particular, one has $(s \circ g)(1) = 1$, from which it follows that

$$1 = (s \circ g)(1) = s(g(1)) = g(1) + 1,$$

in which case $g(1) = 0 \notin \mathbb{N}$, which is a contradiction. So no such right inverse g exists.

Now, fix $m \in \mathbb{N}$, and define $f_m : \mathbb{N} \to \mathbb{N}$ by

$$f_m(n) = \begin{cases} m - 1 & \text{if } n \neq 1, \\ m & \text{otherwise.} \end{cases}$$

Then, for any $n \in \mathbb{N}$, one has

$$(f_m \circ s)(n) = f_m(s(n)) = f_m(n + 1) = (n + 1) - 1 = n,$$

so f_m is a left inverse of s. As m can be chosen arbitrarily from $\mathbb{N}$, we have in fact defined a countable family of left inverses.

Problem 2.1. Make a multiplication table for the symmetric group S_3.

Solution. The standard presentation for the symmetric group S_3, given in (2.2.7) in Artin, is

$$S_3 = \langle x, y \mid x^3 = 1 = y^2,\ yx = x^2y \rangle = \{1, x, x^2, y, xy, x^2y\},$$

where $x = (123)$ and $y = (12)$. Using these defining relations, we compute the multiplication table for S_3.

$\circ$	1	x	x^2	y	xy	x^2y
1	1	x	x^2	y	xy	x^2y
x	x	x^2	1	xy	x^2y	y
x^2	x^2	1	x	x^2y	y	xy
y	y	x^2y	xy	1	x^2	x
xy	xy	y	x^2y	x	1	x^2
x^2y	x^2y	xy	y	x^2	x	1

Problem 4.3. Let a and b be elements of a group G. Prove that ab and ba have the same order.

Solution. We begin with a lemma.

Lemma. For any $n \in \mathbb{N}$,

$$(ab)^n = a(ba)^{n-1}b.$$

Proof. We proceed by induction on n. When $n = 1$, we find that $(ab)^1 = ab = aeb = a(ba)^{1-1}b$. Suppose inductively that $(ab)^k = a(ba)^{k-1}b$ for some fixed $k \geq 1$. It then follows that

$$(ab)^{k+1} = (ab)^k(ab) = (a(ba)^{k-1}b)(ab) = a((ba)^{k-1}(ba))b = a(ba)^k b,$$

which closes the induction. ■

Now, for any $n \in \mathbb{N}$, we have $(ab)^n = e$ if and only if $a(ba)^{n-1}b = e$, which is true if and only if $(ba)^{n-1} = a^{-1}b^{-1} = (ba)^{-1}$, which is true if and only if $(ba)^n = e$. So ab has finite order if and only if ba has finite order, hence ab has infinite order if and only if ba has infinite order. Furthermore, if ab and ba have finite order, then the forward direction implies that the order of ab divides the order of ba and the backward direction that the order of ba divides the order of ab. As $|ab|$ and $|ba|$ are positive, we then conclude that $|ab| = |ba|$.

Problem 5.1. Let $\varphi : G \to G'$ be a surjective homomorphim. Prove that if G is cyclic, then G' is cyclic, and if G is abelian, then G' is abelian.

Solution. Suppose that G is cyclic. So there exists $a \in G$ such that $G = \langle a \rangle$. Fix $y' \in G'$. As φ is surjective, there exists $x' \in G$ such that $\varphi(x') = y'$. As G is cyclic, there exists $m \in \mathbb{Z}$ such that $x' = a^m$. Then

$$y' = \varphi(x') = \varphi(a^m) = \varphi(a)^m,$$

so $y' \in \langle \varphi(a) \rangle$, hence $\langle \varphi(a) \rangle \supseteq G'$. As $\langle \varphi(a) \rangle \subseteq G'$ by definition, we conclude that $\langle \varphi(a) \rangle = G'$, so G' is cyclic.

Next, let $x', y' \in G$. By surjectivity of φ, there exist $x, y \in G$ such that $\varphi(x) = x'$ and $\varphi(y) = y'$. As G is abelian, we find that

$$x'y' = \varphi(x)\varphi(y) = \varphi(xy) = \varphi(yx) = \varphi(y)\varphi(x) = y'x',$$

so G' is abelian, as required.

Problem 5.2. Prove that the intersection of $K \cap H$ of subgroups of a group G is a subgroup of H, and that if K is a normal subgroup of G, then $K \cap H$ is a normal subgroup of H.

Proof. We have $K \cap H \subseteq G$ by definition $K, H \subseteq G$. Let $x, y \in K \cap H$. Then $x, y \in K$ and $x, y \in H$. As K and H are closed under composition, we have $xy \in K$ and $xy \in H$, so $xy \in K \cap H$. As K and H are subgroups, they contain the identity element of G, so $e \in K \cap H$. Finally, given $x \in K \cap H \subseteq G$, there exists an inverse $x^{-1} \in G$. As K and H are closed under inversion, we have $x^{-1} \in K$ and $x^{-1} \in H$, so $x^{-1} \in K \cap H$. So $K \cap H$ is a subgroup of G.

Suppose now that K is a normal subgroup of G. Let $a \in K \cap H$ and $b \in H$. Then $a \in H$, $b \in H$, and $b^{-1} \in H$, so $bab^{-1} \in H$. Furthermore, one has $a \in K$, so because K is a normal subgroup of $G \ni b$, we have $bab^{-1} \in K$. So $bab^{-1} \in K \cap H$, so $K \cap H$ is a normal subgroup of H.

Problem 6.1. Let G' be the group of real matrices of the form $\begin{bmatrix} 1 & x \\ & 1 \end{bmatrix}$. Is the map $\mathbb{R}^+ \to G'$ that sends x to this matrix an isomorphism?

Solution. Define $\varphi : \mathbb{R}^+ \to G'$ by $\varphi(x) = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$. I claim that φ is an isomorphism. First, if $\varphi(x) = \varphi(y)$ for $x, y \in \mathbb{R}$, then $\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix}$. Equating entries then yields $x = y$, so φ is injective. Second, given $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \in G'$, we have $\varphi(a) = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$, so φ is surjective and hence bijective. Finally, we will show that φ is a homomorphism. For any $g, h \in \mathbb{R}$, we find that

$$\varphi(g + h) = \begin{bmatrix} 1 & g+h \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & g \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix} = \varphi(g)\varphi(h),$$

so φ is a homomorphism and hence an isomorphism, hence $\mathbb{R}^+ \cong G'$, as required.

Problem 6.4. Prove that in a group, the products ab and ba are conjugate elements.

Solution. Let $a, b \in G$. We have

$$ab = e(ab) = \left(b^{-1}b\right)(ab) = b^{-1}(ba)b,$$

where $b = \left(b^{-1}\right)^{-1}$, so ab and ba are conjugate elements.