Dummit & Foote Ch. 3.1: Quotient Groups and Homomorphisms

Scott Donaldson

Aug. - Sep. 2023

Let G and H be groups.

1. (9/1/23)

Let $\varphi : G \to H$ be a homomorphism and let $E \leq H$. Prove that $\varphi^{-1}(E) \leq G$ (i.e., the preimage or pullback of a subgroup under a homomorphism is a subgroup). If $E \trianglelefteq H$ prove that $\varphi^{-1}(E) \trianglelefteq G$. Deduce that ker $\varphi \trianglelefteq G$.

Proof. Let $x, y \in \varphi^{-1}(E) \subseteq G$. Suppose that $\varphi(x) = a, \varphi(y) = b, a, b \in E \leq H$. Since φ is a homomorphism, we have $\varphi(y^{-1}) = \varphi(y)^{-1} = b^{-1}$. Then:

$$\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y)^{-1} = ab^{-1} \in E,$$

which implies that $xy^{-1} \in \varphi^{-1}(E)$. It follows that, by the subgroup criterion, $\varphi^{-1}(E) \leq G$.

Next, let $E \trianglelefteq H$ (to show that $\varphi^{-1}(E) \trianglelefteq G$). Again let $x \in \varphi^{-1}(E) \leq G$ and suppose $\varphi(x) = a$. Now for some $g \in G$ (not necessarily in $\varphi^{-1}(E)$), consider $\varphi(gxg^{-1})$. Suppose also that $\varphi(g) = h \in H$. Because E is normal in H and $a \in E$, we have $hah^{-1} \in E$. Then:

$$\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} = hah^{-1} \in E,$$

which implies that $gxg^{-1} \in \varphi^{-1}(E)$. Since the conjugate of any element of $\varphi^{-1}(E)$ by any other element of G lies in $\varphi^{-1}(E)$, we therefore conclude that $\varphi^{-1}(E) \trianglelefteq G$.

Finally, we note that ker $\varphi = \{g \in G \mid \varphi(g) = 1_H\}$. Since the trivial subgroup consisting of the identity of H is normal (the conjugate of 1_H by any element of H is 1_H), we therefore have $\varphi^{-1}(\{1_H\}) = \ker \varphi \trianglelefteq G$. □

2. (8/23/23)

Let $\varphi : G \to H$ be a homomorphism of groups with kernel K and let $a, b \in \varphi(G)$. Let $X \in G/K$ be the fiber above a and Y be the fiber above b, i.e.,

$X = \varphi^{-1}(a), Y = \varphi^{-1}(b)$. Fix an element $x \in X$ (so $\varphi(x) = a$). Prove that if $XY = Z$ in the quotient group G/K and z is any member of Z, then there is some $y \in Y$ such that $xy = z$.

Proof. We know that, for any $x \in X, y \in Y$, $\varphi(x) = a$ and $\varphi(y) = b$. Since φ is a homomorphism, it follows that $\varphi(xy) = \varphi(x)\varphi(y) = ab$, and so the image of any element of $XY = Z$ under φ is $ab \in H$.

Next, consider the element $x^{-1}z \in G$, as well as its image under φ. Since φ is a homomorphism, we have $\varphi(x^{-1}) = \varphi(x)^{-1}$. So $\varphi(x^{-1}z) = \varphi(x^{-1})\varphi(z) = \varphi(x)^{-1}\varphi(z) = a^{-1}ab = b$. The set Y consists of all elements of G whose image under φ is b, and so we must have $x^{-1}z \in Y$.

Now if we fix some element $x \in X$, then for any $z \in Z$, we have $x^{-1}z \in Y$ such that its product with x is z: $xx^{-1}z = z$. $\square$

3. (8/23/23)

Let A be an abelian group and let B be a subgroup of A. Prove that A/B is abelian. Give an example of a non-abelian group G containing a proper normal subgroup N such that G/N is abelian.

Proof. Because A is abelian, all subgroups of A are normal, so A/B is well-defined for every $B \leq A$.

Let $C, D \in A/B$ with $C = cB$ and $D = dB$ for some $c, d \in A$. Then:

$$CD = (cB)(dB) = (cd)B = (dc)B = (dB)(cB) = DC,$$

which implies that A/B is abelian.

Now if we let G be the dihedral group D_8, then G is non-abelian. Let N be the cyclic subgroup generated by $r : \{1, r, r^2, r^3\}$. The only coset of N is sN; together these two sets cover G. Then $G/N = \{N, sN\}$. There is only one group of order 2 up to isomorphism, and it is abelian. Thus G/N is abelian. $\square$

4. (8/23/23)

Prove that in the quotient group G/N, $(gN)^\alpha = (g^\alpha)N$ for all $\alpha \in \mathbb{Z}$.

Proof. We start by induction: In the base case, $\alpha = 1$, we have $(gN)^1 = gN = (g^1)N$. Next, suppose that for some $\alpha > 1$, we have $(gN)^\alpha = (g^\alpha)N$. Then:

$$(gN)^{\alpha+1} = (gN)^\alpha gN = g^\alpha N \cdot gN = (g^{\alpha+1})N,$$

as desired. We have now proven that $(gN)^\alpha = (g^\alpha)N$ for $\alpha \geq 1$.

Next, consider $(gN)^\alpha(gN)^{-\alpha}$, where $\alpha \geq 1$. In the quotient group G/N, for any subset $X \in G/N$, we must have $X^\alpha X^{-\alpha} = N$ (the identity of G/N), so $(gN)^\alpha(gN)^{-\alpha} = N$. From above, $(gN)^\alpha = (g^\alpha)N$, so $(g^\alpha)N \cdot (gN)^{-\alpha} = N$. Also, from the operation on left cosets, we know that $N = (g^\alpha)N \cdot (g^{-\alpha})N$.

Since both $(g^\alpha)N \cdot (gN)^{-\alpha} = N$ and $(g^\alpha)N \cdot (g^{-\alpha})N = N$, we must have $(gN)^{-\alpha} = (g^{-\alpha})N$. We have now proven for all nonzero integers.

Finally, we note that $(gN)^0 = N$ (the identity of G/N) and that $(g^0)N = eN = N$, so $(gN)^0 = (g^0)N$. This concludes the proof that $(gN)^\alpha = (g^\alpha)N$ for all $\alpha \in \mathbb{Z}$. $\square$

5. (8/23/23)

Use the preceding exercise to prove that the order of the element gN in G/N is n, where n is the smallest positive integer such that $g^n \in N$ (and gN has infinite order if no such positive integer exists). Give an example to show that the order of gN in G/N may be strictly smaller than the order of g in G.

Proof. Let $gN \in G/N$, and let n be the smallest positive integer such that $g^n \in N$. Suppose that $g^n = h \in N$.

From Exercise 4., $(gN)^n = (g^n)N = hN = N$ (because $h \in N$), so the order of gN must divide n.

Suppose (toward contradiction) that the order of gN is k, where $k < n$. Then $(gN)^k = (g^k)N = N$, which implies that g^k lies in N, contradicting our assumption that n is the smallest such positive integer. Therefore the order of gN is n.

If there is no positive integer n such that $g^n \in N$, then for all $k \in \mathbb{Z}^+$, we have $(gN)^k = (g^k)N \neq N$, so gN has infinite order.

As an example where $|gN| < |g|$, let $G = Z_9 = \langle x \rangle$ and let $N = \langle x^3 \rangle$. Because all cyclic groups are abelian, N is normal in G, and so G/N is well-defined. The quotient group G/N contains three elements: N, xN, and $(x^2)N$. The element $xN \in G/N$ has order 3: $(xN)^3 = (x^3)N = N$ (because $x^3 \in N$). However, the generating element $x \in G$ has order 9. $\square$

6. (8/24/23)

Define $\varphi : \mathbb{R}^\times \to \{\pm 1\}$ by letting $\varphi(x)$ be x divided by the absolute value of x. Describe the fibers of φ and prove that φ is a homomorphism.

Proof. We consider the two cases where $x < 0$ and $x > 0$ (0 is not an element of $\mathbb{R}^\times$). If $x > 0$, then $\varphi(x) = x/|x| = x/x = 1$. If $x < 0$, then $\varphi(x) = x/|x| = x/-x = -1$. Therefore the fiber above -1 is every negative real number and the fiber above 1 is every positive real number.

To show that φ is a homomorphism, we let $x, y \in \mathbb{R}^\times$ and again consider the different cases: Where x and y are both positive, where they are both negative, and where one is positive and the other negative.

If both x and y are positive, then $\varphi(x)\varphi(y) = 1 \cdot 1 = 1$ and $\varphi(xy) = \frac{xy}{|xy|} = \frac{xy}{xy} = 1$, so $\varphi(x)\varphi(y) = \varphi(xy)$.

If both x and y are negative, then $\varphi(x)\varphi(y) = -1 \cdot -1 = 1$ and $\varphi(xy) = \frac{xy}{|xy|} = \frac{xy}{xy} = 1$, so $\varphi(x)\varphi(y) = \varphi(xy)$.

Suppose x is positive and y is negative. Then $\varphi(x)\varphi(y) = 1 \cdot -1 = -1$ and $\varphi(xy) = \frac{xy}{|xy|} = \frac{xy}{-xy} = -1$, so $\varphi(x)\varphi(y) = \varphi(xy)$.

Thus, in every case of $x, y \in \mathbb{R}^\times$, we have $\varphi(x)\varphi(y) = \varphi(xy)$, and φ is thus a homomorphism. $\square$

7. (8/24/23)

Define $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x + y$. Prove that π is a surjective homomorphism and the describe the kernel and fibers of π geometrically.

Proof. First, to show that π is surjective, let $z \in \mathbb{R}$. Now $z = z + 0$, so $(z, 0)$ is an element of $\mathbb{R}^2$ such that $\pi((z, 0)) = z + 0 = z$.

Next, to show that π is a homomorphism, let $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$. We have $\pi((x_1, y_1) + (x_2, y_2)) = \pi((x_1 + x_2, y_1 + y_2)) = x_1 + x_2 + y_1 + y_2$, and $\pi((x_1, y_1)) + \pi((x_2, y_2)) = x_1 + y_1 + x_2 + y_2$. By the commutativity of addition in $\mathbb{R}$, these are equal to each other, and so π is a surjective homomorphism.

The kernel of π consists of all points $(x, y) \in \mathbb{R}^2$ such that $x + y = 0$, that is, the diagonal line running from the upper-left to the bottom-right of the Cartesian plane. Geometrically, the fibers of π are translations of this line, such that for any $z \in \mathbb{R}$, the fiber of π above z is the diagonal line intersecting both $(z, 0)$ and $(0, z)$. $\square$

8. (8/24/23)

Let $\varphi : \mathbb{R}^\times \to \mathbb{R}^\times$ be the map sending x to the absolute value of x. Prove that φ is a homomorphism and find the image of φ. Describe the kernel and the fibers of φ.

Proof. Let $x, y \in \mathbb{R}^\times$ (so $x \neq 0, y \neq 0$). If both x and y are positive or both are negative, then:

$$\varphi(xy) = |xy| = |x||y| = \varphi(x)\varphi(y),$$

and if x is positive and y is negative, then:

$$\varphi(xy) = |xy| = x(-y) = |x||y| = \varphi(x)\varphi(y),$$

so φ is a homomorphism.

The image of φ consists of every positive real number. The kernel of φ is the set $\{x \in \mathbb{R}^\times \mid |x| = 1\}$, that is, $\{\pm 1\}$. For a given element $z > 0$, the fiber of φ above z is the set $\{\pm z\}$. $\square$

9. (8/25/23)

Define $\varphi : \mathbb{C}^\times \to \mathbb{R}^\times$ by $\varphi(a + bi) = a^2 + b^2$. Prove that φ is a homomorphism and find the image of φ. Describe the kernel and the fibers of φ geometrically (as subsets of the plane).

Proof. To show that φ is a homomorphism, let $z_1 = a_1 + b_1 i, z_2 = a_2 + b_2 i \in \mathbb{C}^\times$. We calculate:

$$\begin{aligned}
\varphi(z_1 z_2) &= \varphi((a_1 + b_1 i)(a_2 + b_2 i)) \\
&= \varphi((a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1) i) \\
&= (a_1 a_2 - b_1 b_2)^2 + (a_1 b_2 + a_2 b_1)^2 \\
&= a_1^2 a_2^2 - 2a_1 a_2 b_1 b_2 + b_1^2 b_2^2 + a_1^2 b_2^2 + 2a_1 a_2 b_1 b_2 + a_2^2 b_1^2 \\
&= a_1^2 a_2^2 + b_1^2 b_2^2 + a_1^2 b_2^2 + a_2^2 b_1^2, \text{ and} \\
\varphi(z_1)\varphi(z_2) &= \varphi(a_1 + b_1 i)\varphi(a_2 + b_2 i) = (a_1^2 + b_1^2)(a_2^2 + b_2^2) \\
&= a_1^2 a_2^2 + b_1^2 b_2^2 + a_1^2 b_2^2 + a_2^2 b_1^2,
\end{aligned}$$

which proves that φ is a homomorphism.

The image of a complex number $a + bi$ under φ is $a^2 + b^2$, which is always non-negative because it is the sum of two non-negative numbers. Since both $\mathbb{C}^\times$ and $\mathbb{R}^\times$ exclude 0, the image of φ is therefore all positive real numbers.

The kernel of φ are those complex numbers whose image under φ is 1. Geometrically, φ is a map from a point in the complex plane to its length, or distance from zero. Therefore the kernel of φ is the unit circle in the complex plane. The fibers of a given positive real number x is the circle of radius x centered at the origin in the complex plane. □

10. (8/28/23)

Let $\varphi : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ by $\varphi(\overline{a}) = \overline{a}$. Show that this is a well-defined, surjective homomorphism and describe its fibers and kernel explicitly (showing that φ is well-defined involves the fact that $\overline{a}$ has a different meaning in the domain and range of φ).

Proof. The map φ is well-defined because it assigns to each member of $\mathbb{Z}/8\mathbb{Z}$ a single, unique element of $\mathbb{Z}/4\mathbb{Z}$. Let $a \in \{0, ...7\}$ be equal to $\overline{a}$ mod 8. Then we have $\varphi(\overline{a}) = \varphi(a)$. Further, φ assigns each $a \in \{0, ...7\}$ to a mod 4; that is, it assigns 0 and 4 to 0, 1 and 5 to 1, 2 and 6 to 2, and 3 and 7 to 3. This also shows that φ is surjective, since each $\overline{a} \cong \mathbb{Z}/4\mathbb{Z}$ (represented by $a = \overline{a}$ mod 4) has a preimage in $\mathbb{Z}/8\mathbb{Z}$.

The kernel of φ is $\{0, 4\} \leq \mathbb{Z}/8\mathbb{Z}$, and the fiber of any $a \in \mathbb{Z}/4\mathbb{Z}$ is the tuple $\{a, a + 4\}$. □

11. (8/28/23)

Let F be a field and let $G = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in F, ac \neq 0\} \leq GL_2(F)$.

(a) Prove that the map $\varphi : \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto a$ is a surjective homomorphism from G onto $F^\times$ (recall that $F^\times$ is the multiplicative group of nonzero elements in F). Describe the fibers and kernel of φ.

Proof. To show that φ is surjective, let $a \in F^\times$ (so $a \neq 0$). Then we have $\varphi(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}) = a$, so φ is onto.

Next, to show that it is a homomorphism, we note that:

$$\varphi(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} d & e \\ 0 & f \end{pmatrix}) = \varphi(\begin{pmatrix} ad & ae + bf \\ 0 & cf \end{pmatrix}) = ad = \varphi(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix})\varphi(\begin{pmatrix} d & e \\ 0 & f \end{pmatrix}),$$

so φ is also a homomorphism.

The kernel of φ is $\{\begin{pmatrix} 1 & b \\ 0 & c \end{pmatrix} \mid b, c \in F, c \neq 0\}$, and the fiber of φ over a given element $a \in F^\times$ is $\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid b, c \in F, c \neq 0\}$. □

(b) Prove that the map $\psi : \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a, c)$ is a surjective homomorphism from G onto $F^\times \times F^\times$. Describe the fibers and kernel of ψ.

Proof. To show that ψ is surjective, let $(a, c) \in F^\times \times F^\times$ (so $a, c \neq 0$). Then we have $\psi(\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}) = (a, c)$, so ψ is onto.

Next, to show that it is a homomorphism, we note that:

$$\begin{aligned}\psi(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} d & e \\ 0 & f \end{pmatrix}) &= \psi(\begin{pmatrix} ad & ae + bf \\ 0 & cf \end{pmatrix}) = (ad, cf) \\ &= (a, c)(d, f) = \psi(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix})\psi(\begin{pmatrix} d & e \\ 0 & f \end{pmatrix}),\end{aligned}$$

so ψ is also a homomorphism.

The kernel of ψ is the preimage of $(1, 1)$, that is, $\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in F\}$, and the fiber of ψ over a given element $(a, c) \in F^\times \times F^\times$ is $\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid b \in F\}$. □

(c) Let $H = \{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in F\}$. Prove that H is isomorphic to the additive group F.

Proof. As usual, to show that H is isomorphic to the additive group F, we must show that there exists a bijective homomorphism $\varphi : H \to F$. Define φ by $\varphi(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}) = b$. We will show that it is an isomorphism.

First, φ is injective: Suppose that $\varphi(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}) = \varphi(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}) = c$. Then we have $a = c$ and $b = c$, so the two matrices are the same, and φ is injective.

Next, φ is surjective: Let $b \in F$. Then we have $\varphi(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}) = b$.

Finally, φ is a homomorphism:

$$\varphi(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}) = \varphi(\begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}) = a+b = \varphi(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}) + \varphi(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}).$$

□

12. (8/30/23)

Let G be the additive group of real numbers, let H be the multiplicative group of complex numbers of absolute value 1 (the unit circle S^1 in the complex plane) and let $\varphi : G \to H$ be the homomorphism $\varphi : r \mapsto e^{2\pi i r}$. Draw the points on the real line which lie in the kernel of φ. Describe similarly the elements in the fibers of φ above the points -1, i, and $e^{4\pi i/3}$ of H.

Proof. The kernel of φ is the set $\{r \in \mathbb{R} \mid e^{2\pi i r} = 1\}$. Recall that $e^{2\pi i r} = \cos 2\pi r + i \sin 2\pi r$, so the values of r for which $e^{2\pi i r} = 1$ are those where $\cos 2\pi r = 1$, that is, all of the integers.

We similarly obtain the fiber of φ above -1 by considering when $\cos 2\pi r = -1$, which occurs when $r = 1/2, 3/2, 5/2, ...$, that is, $r \in \{n + \frac{1}{2} \mid n \in \mathbb{Z}\}$. For the fiber above i, we must have $\sin 2\pi r = 1$, which occurs when $r = 1/4, 5/4, 9/4, ...$, that is, $r \in \{n + \frac{1}{4} \mid n \in \mathbb{Z}\}$. Finally, we have $4\pi/3 = \frac{2}{3} \cdot 2\pi$, so the fiber above $e^{4\pi i/3}$ is $\{n + \frac{2}{3} \mid n \in \mathbb{Z}\}$.

We can also write these as cosets of $\mathbb{Z}$, so the fibers are $\frac{1}{2} + \mathbb{Z}$, $\frac{1}{4} + \mathbb{Z}$, and $\frac{2}{3} + \mathbb{Z}$, respectively. □

13. (8/31/23)

Repeat the preceding exercise with the map φ replaced by the map $\varphi : r \mapsto e^{4\pi i r}$.

Proof. In this case, the kernel of φ consists of values of r for which $e^{4\pi i r} = 1 \Rightarrow \cos 4\pi r = 1$. The period is now halved, so this occurs when $r \in \{1/2, 1, 3/2, ...\}$; the kernel is $\{\frac{n}{2} \mid n \in \mathbb{Z}\}$.

The fiber of φ above -1 has $\cos 4\pi r = -1$, when $r = 1/4, 3/4, 5/4, ...$, that is, $r \in \{\frac{1}{4} + \frac{n}{2} \mid n \in \mathbb{Z}\}$. Above i, we have $\sin 4\pi r = 1$, so $r \in \{\frac{1}{8}, \frac{5}{8}, ...\}$, and the fiber is $\{\frac{1}{8} + \frac{n}{2} \mid n \in \mathbb{Z}\}$. Finally, above $4\pi/3$, the fiber is $\{\frac{1}{3} + \frac{n}{2} \mid n \in \mathbb{Z}\}$.

If we denote the kernel in this exercise as $\frac{1}{2}\mathbb{Z}$, then as cosets, the fibers are $\frac{1}{4} + \frac{1}{2}\mathbb{Z}$, $\frac{1}{8} + \frac{1}{2}\mathbb{Z}$, and $\frac{1}{3} + \frac{1}{2}\mathbb{Z}$, respectively. □

14. (8/31/23)

Consider the additive quotient group $\mathbb{Q}/\mathbb{Z}$.

(a) Show that every coset of $\mathbb{Z}$ in $\mathbb{Q}$ contains exactly one representative $q \in \mathbb{Q}$ in the range $0 \leq q < 1$.

Proof. The rational numbers under addition constitutes an abelian group, so $\mathbb{Z}$ is a normal subgroup of $\mathbb{Q}$, and $\mathbb{Q}/\mathbb{Z}$ is therefore well-defined. The elements of the quotient group $\mathbb{Q}/\mathbb{Z}$ are cosets of $\mathbb{Z}$ in $\mathbb{Q}$, for example, $\mathbb{Z}$ itself (the identity), as well as $\frac{1}{2} + \mathbb{Z}$, $\frac{7}{4} + \mathbb{Z}$, and so on.

Let $q + \mathbb{Z}$ be a coset of $\mathbb{Z}$ (for arbitrary $q \in \mathbb{Q}$). If $q > 1$, then let $n \in \mathbb{Z}$ be the largest integer such that $q - n \geq 0$ (such an integer exists by the well-ordering property). Then $q - n$ is the unique representative for $q + \mathbb{Z}$ in the range $[0, 1)$, since $q - n - 1 < 0$ and $q - n + 1 > 1$. Similarly, if $q < 0$, there exists a unique n such that $0 \leq q + n < 1$. Finally, if $0 \leq q < 1$, then q itself is the unique representative for $q + \mathbb{Z}$ lying between 0 (inclusive) and 1 (exclusive). □

(b) Show that every element of $\mathbb{Q}/\mathbb{Z}$ has finite order but that there are elements of arbitrarily large order.

Proof. Let $\frac{a}{b} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$ (with $0 \leq \frac{a}{b} < 1$, as above, and suppose that $\frac{a}{b}$ is in lowest terms). Then we have:

$$\underbrace{(\frac{a}{b} + \mathbb{Z}) + ... + (\frac{a}{b} + \mathbb{Z})}_{b \text{ times}} = \underbrace{(\frac{a}{b} + ... + \frac{a}{b})}_{b \text{ times}} + \mathbb{Z} = a + \mathbb{Z} = \mathbb{Z},$$

so the order of $\frac{a}{b} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$ is at most b, and it therefore has finite order.

However, given a coset $\frac{1}{b} + \mathbb{Z}$ of order b, there always exists an element of higher order, for example $\frac{1}{b+1} + \mathbb{Z}$ and $\frac{1}{2b} + \mathbb{Z}$, which have order $b + 1$ and $2b$, respectively. □

(c) Show that $\mathbb{Q}/\mathbb{Z}$ is the torsion subgroup of $\mathbb{R}/\mathbb{Z}$.

Proof. Recall that the torsion subgroup of $\mathbb{R}/\mathbb{Z}$ is the set of elements of $\mathbb{R}/\mathbb{Z}$ of finite order (by Chapter 2.1, Exercise 6., this set is a subgroup when the parent group is abelian).

First, let $q + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$. Since rational numbers are also real numbers, $q + \mathbb{Z}$ also lies in $\mathbb{R}/\mathbb{Z}$. From 14.b), it has finite order. Therefore it is an element of the torsion subgroup of $\mathbb{R}/\mathbb{Z}$.

Next, let $x + \mathbb{Z}$ be an element of the torsion subgroup of $\mathbb{R}/\mathbb{Z}$. Suppose that $|x + \mathbb{Z}| = n < \infty$. Then we have:

$$\underbrace{(x + \mathbb{Z}) + ... + (x + \mathbb{Z})}_{n \text{ times}} = \underbrace{(x + ... + x)}_{n \text{ times}} + \mathbb{Z} = nx + \mathbb{Z} = \mathbb{Z},$$

which implies that nx is an integer. Suppose that $nx = m \in \mathbb{Z}$. Then $x = m/n$, and so we have $x \in \mathbb{Q}$, which implies that $x + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$.

Therefore, because inclusion in one implies inclusion in the other and vice-versa, these groups are equal. □

(d) Prove that $\mathbb{Q}/\mathbb{Z}$ is isomorphic to the multiplicative group of roots of unity in $\mathbb{C}^\times$.

Proof. Let $\varphi : \mathbb{Q}/\mathbb{Z} \to \mathbb{C}^\times$ be defined by $\varphi(r+\mathbb{Z}) = e^{2\pi ir}$, where $0 \leq r < 1$. We will show that φ is a bijective homomorphism, and that the groups are thus isomorphic to each other.

First, to show that φ is a homomorphism, note that:

$$\varphi((q + \mathbb{Z}) + (r + \mathbb{Z})) = \varphi((q + r) + \mathbb{Z}) = e^{2\pi i(q+r)}, \text{ and}$$
$$\varphi(q + \mathbb{Z})\varphi(r + \mathbb{Z}) = e^{2\pi iq}e^{2\pi ir} = e^{2\pi iq+2\pi ir} = e^{2\pi i(q+r)},$$

as desired.

Next, φ is one-to-one: Suppose $e^{2\pi ir} = \varphi(r + \mathbb{Z}) = \varphi(q + \mathbb{Z})$ for some $r, q \in [0, 1)$. In fact, there are many possible rational numbers fulfilling this if we open the range to all of $\mathbb{Q}$; however, because the period of $e^{2\pi ir}$ is 1, there is only one unique value in the range $[0, 1)$, so we must have $r = q$. Therefore φ is injective.

Finally, φ is surjective: Let z be a root of unity with order n. Then z can be expressed as $e^{2\pi it/n}$ for some $t \in \{0, 1, ..., n - 1\}$. By definition of φ, the rational number $t/n \in [0, 1)$ has $\varphi(t/n) = e^{2\pi it/n} = z$. Thus φ is a bijective homomorphism, and so $\mathbb{Q}/\mathbb{Z}$ is isomorphic to the roots of unity in $\mathbb{C}^\times$. □

15. (9/1/23)

Prove that the quotient of a divisible abelian group by any proper subgroup is also divisible. Deduce that $\mathbb{Q}/\mathbb{Z}$ is divisible.

Proof. Let A be a divisible abelian group and let B be a proper subgroup of A. Since A is abelian, all of its subgroups are normal, so the quotient group A/B is well-defined.

Let $aB \in A/B$ and let $k > 0$. Since A is divisible, there exists an $x \in A$ such that $x^k = a$. Then we have $aB = (x^k)B = (xB)^k$ for $xB \in A/B$, so aB has a k-th root in A/B. Therefore A/B is divisible.

Note that the rational numbers under addition form a divisible abelian group (from Ch. 2.4, Exercise 19.) and the integers are a proper subgroup of the rational numbers. It follows that the quotient group $\mathbb{Q}/\mathbb{Z}$ is divisible. $\square$