TheNumbersBook.com 2010

Dummit & Foote (3.1) 1, 6, 7, 9, 14, 24, 40, 41

3.1.1 Let $\varphi : G \to H$ be a homomorphism and let E be a subgroup of 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 $\ker \varphi \trianglelefteq G$.

We prove that $\varphi^{-1}(E)$ is nonempty, closed under inverses and products:

(1) Since E is a subgroup of H, then $e_H \in E$ and so $e_G = \phi^{-1}(e_H)$ because identities map to identities.

(2) $\phi^{-1}(E)$ is closed under multiplication: Let $g, g' \in \phi^{-1}(E)$. Then $\phi(g), \phi(g') \in E$ (because if g, g' are in the preimage of E, then they must have been in the image of E in the first place). Since E is a subgroup, it is closed under multiplication. Thus, $\phi(g)\phi(g') \in E$. Since ϕ is a homomorphism, we have that $\phi(gg') \in E$ and so $gg' \in \phi^{-1}(E)$.

(3) Finally, let $g \in \phi^{-1}(E)$. Then $\phi(g) \in E$ and since E is a subgroup of H, $\phi(g)^{-1} \in E$. Specifically, since ϕ is a homomorphism, $\phi(g^{-1}) \in E$ and so $g^{-1} \in \phi^{-1}(E)$, as desired.

Thus, $\phi^{-1}(E) \subseteq G$.

Since E is normal, $E = \phi(g^{-1})E\phi(g) = \phi(g)^{-1}E\phi(g)$. Taking the inverse map of both sides yields

$$g^{-1}\phi^{-1}(E)g = \phi^{-1}(E)$$

This implies that $\phi^{-1}(E)$ is normal.

Finally, we deduce that $\ker(\phi) \trianglelefteq G$. Note that $\phi(\ker(\phi)) = \{0\}$ as $\ker(\phi) = \{x \in G | \phi(x) = 0\}$. Since 0 is trivially a normal subgroup of H, we have that $\phi^{-1}(\phi(\ker(\phi))) = \ker(\phi)$ is a normal subgroup of G. ∎

3.1.6 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.

The fibers are as follows: all elements $x \in \mathbb{R}^+$ will map to $+1$ and all elements $x \in \mathbb{R}^-$ will map to -1.

We now prove that φ is a homomorphism. First, note that the binary operation is multiplication. Let $a, b \in \mathbb{R}$:

$$\begin{aligned}\varphi(ab) &= \frac{ab}{|ab|} \\ &= \frac{a}{|a|}\frac{b}{|b|} \text{ (Property of absolute value)} \\ &= \varphi(a)\varphi(b)\end{aligned}$$

So φ satisfies the property of homomorphism. ∎

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

Consider $+$ to be the componentwise addition. Then for $(a,b),(c,d) \in \mathbb{R}^2$,

$$\begin{aligned}\pi((a,b)+(c,d)) &= \pi((a+c, b+d)) \\ &= (a+c)+(b+d) \\ &= (a+b)+(c+d) \text{ ($\mathbb{R}$ is commutative)} \\ &= \pi((a,b)) + \pi((c,d))\end{aligned}$$

Now note that for any $x + y \in \mathbb{R}$, consider the point $(x,y) \in \mathbb{R}^2$. Clearly, $\pi((x,y)) = x + y$, so π is surjective.

The fiber of π are the equations of the form $x + y = m$ where m is some real number. Interestingly, there is an uncountable set of points (x,y) that map m (i.e. there is an uncountable number of ways to write m using two real numbers). Notice how this partitions $\mathbb{R}$. With regard to the kernel, note that $0 \in \mathbb{R}$ is the additive identity. Thus, the fiber corresponding to the kernel is $x + y = 0$, or all points in $\mathbb{R}^2$ of the form $(x, -x)$. ∎

3.1.9 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).

Let $a + bi, c + di \in \mathbb{C}$:

$$\begin{aligned}\varphi((a+bi)(c+di)) &= \varphi(ac + adi + bci + bdi^2) \\ &= \varphi((ac-bd)+(ad+bc)i) \\ &= (ac-bd)^2 + (ad+bc)^2 \\ &= a^2c^2 - 2acbd + b^2d^2 + a^2d^2 + 2adbc + b^2c^2 \\ &= a^2(c^2+d^2) + b^2(c^2+d^2) \\ &= (a^2+b^2)(c^2+d^2) \\ &= \varphi(a+bi)\varphi(c+di)\end{aligned}$$

The image of φ is all the non-negative real number, which is a subset of $\mathbb{C}$ (why nonnegative? Because $0 \notin \mathbb{C}^{\times}$). The fibers of φ are of the form $a^2 + b^2 = m$ for some positive real number m. In other words, fibers are the circles of radius $\sqrt{m}$. The kernel, then, is a circle of radius 1. ∎

3.1.14 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 $0 \leq q < 1$.

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

(c) Show that $\mathbb{Q}/\mathbb{Z}$ is the torsion subgroup of $\mathbb{R}/\mathbb{Z}$ (cf. Exercise 6, Section 2.1).

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

(a) Consider an arbitrary coset $q + \mathbb{Z}$ where $q \in \mathbb{Q}$. We can write q *uniquely* in terms of its integral and fractional part to get:

$$q = int(q) + frac(q)$$

(note that $\frac{(}{q})$ is unique). Since $int(q) \in \mathbb{Z}$, we get that $q + \mathbb{Z} = \frac{(}{q}) + \mathbb{Z}$. Since $\frac{(}{q}) \in [0, 1)$, every coset contains exactly one representative in the interval $[0, 1)$.

(b) Recall that $(q + \mathbb{Z}) + (r + \mathbb{Z}) = (q + r + \mathbb{Z})$ and consider an arbitrary coset $q + \mathbb{Z}$. Since $q \in \mathbb{Z}$, we write it as $\frac{a}{b} + \mathbb{Z}$ where $a, b \in \mathbb{Z}$ and are in lowest terms. Note that

$$\begin{aligned}
b(q + \mathbb{Z}) &= b(\frac{a}{b} + \mathbb{Z}) \\
&= (\frac{a}{b} + \mathbb{Z}) + \frac{a}{b} + \mathbb{Z}) + \cdots + (\frac{a}{b} + \mathbb{Z}) \\
&= (b\frac{a}{b} + \mathbb{Z}) \\
&= a + \mathbb{Z} \\
&= \mathbb{Z}
\end{aligned}$$

and it is the smallest such b that yields the identity in $\mathbb{Q}/\mathbb{Z}$. Thus, the order of any coset is simply the denominator, in lowest terms. Clearly, b can get arbitrarily large.

(c) Note that $\mathbb{Q}/\mathbb{Z}$ is a subgroup of $\mathbb{R}/\mathbb{Z}$. Consider any element (a coset in this case) of $\mathbb{R}/\mathbb{Z}$. As seen above, it must be of the form $r + \mathbb{Z}$ where (in this case), $r \in \mathbb{R}$ and $r \in [0, 1)$ for the same reasoning as part a. Now it is easy to verify that there exists an integer k such that $rk \in \mathbb{Z}$ iff $r \in \mathbb{Q}$ (a standard result in analysis). It follows $r + \mathbb{Z}$ has a finite order iff $r \in \mathbb{Q}$. Thus, $\mathbb{Q}/\mathbb{Z}$ are the only subsets of $\mathbb{R}/\mathbb{Z}$ that have finite order. Thus $\mathbb{Q}/\mathbb{Z}$ is a torsion subgroup of $\mathbb{R}/\mathbb{Z}$.

(d) Let $\zeta_m = e^{\frac{2\pi i}{m}}$ and consider the map

$$\phi : \mathbb{Q}/\mathbb{Z} \to \mathbb{C}^\times$$

defined by $\phi(\frac{a}{b} + \mathbb{Z}) = \zeta_b$. We show that ϕ is an isomorphism. First, note that $\ker(\phi) = \{\mathbb{Z}\}$ as the only cosets that go to $\zeta_1 = 1$ is $b = 1$ (or $\mathbb{Z}$) (injectivity). Furthermore, for any root of unity ζ_m^k, we have the corresponding element $\frac{ak}{b} + \mathbb{Z}$ (surjectivity). Thus, ϕ is an isomorphism, as desired.

■

3.1.24 Prove that if $N \trianglelefteq G$ and H is any subgroup of G then $N \cap H \trianglelefteq H$.

Let $k \in N \cap H$. Then $k \in N \trianglelefteq G$. Thus, $g^{-1}kg \in N$ for all $g \in G$ because N is normal. Specifical,y $h^{-1}kh \in N$ for all $h \in H$. On the other hand, $k \in H$ and $h^{-1}kh \in H$ for all $h \in H$ because H is closed. Thus, for any $k \in N \cap H$,

$$h^{-1}kh \in N \cap H$$

for all $h \in H$. Thus, $N \cap H \trianglelefteq H$. ■

3.1.40 Let G be a group, let N be a normal subgroup of G and let $\overline{G} = G/N$. Prove that $\overline{x}$ and $\overline{y}$ commute in $\overline{G}$ if and only if $x^{-1}y^{-1}xy \in N$. (The element $x^{-1}y^{-1}xy$ is called the *commutator* of x and y and is denoted by $[x, y]$.)

($\Rightarrow$) Note that elements of $\overline{G}$ are of the form xN. Now let $\overline{x} = xN, \overline{y} = yN$ be any two elements of $\overline{G}$. Then

$$\overline{xy} = \overline{yx}$$

and so $xyN = (xN)(yN) = (yN)(xN) = yxN$. This implies that $x^{-1}y^{-1}xyN = N$ and so $x^{-1}y^{-1}xy \in N$.

($\Leftarrow$) Note that if $x^{-1}y^{-1}xy \in N$ then $x^{-1}y^{-1}xy$ and 1 are coset representatives of the same coset, namely N. Thus, $x^{-1}y^{-1}xyN = N$ or equivalently $yxN = xyN$. Now consider any $\overline{x} = xN, \overline{y} = yN \in \overline{G}$. Then

$$\begin{aligned}\overline{xy} &= (xN)(yN) \\ &= xyN \\ &= yxN \text{ (because } x^{-1}y^{-1}xy \in N) \\ &= (yN)(xN) \\ &= \overline{yx}\end{aligned}$$

Thus, $\overline{x}, \overline{y}$ commute. ■

3.1.41 Let G be a group. Prove that $N = \langle x^{-1}y^{-1}xy | x, y \in G \rangle$ is a normal subgroup of G and G/N is abelian (N is called the *commutator subgroup* of G).

We want to show that $g^{-1}(x^{-1}y^{-1}xy)g \in N$ for $g \in G$. Using the fact that $gg^{-1} = 1$, we get:

$$\begin{aligned} g^{-1}x^{-1}y^{-1}xyg &= g^{-1}x^{-1}1y^{-1}1x1yg \\ &= g^{-1}x^{-1}gg^{-1}y^{-1}gg^{-1}xgg^{-1}yg \\ &= (g^{-1}xg)^{-1}(g^{-1}yg)^{-1}(g^{-1}xg)(g^{-1}yg) \text{ (Property of inverses)} \\ &= x'^{-1}y'^{-1}x'y' \text{ (for some } x', y' \in G) \\ &\in N \end{aligned}$$

Thus, N is normal. Now note that $x^{-1}y^{-1}xy \in N$ for all $x, y \in G$. By 3.1.40, $\overline{x}, \overline{y}$ commute in G/N. Thus, G/N is abelian. ■