Nathan Bickel
MATH 701: Section 001
Professor: Dr. Tsai
October 17, 2024

MATH 701 Homework 5

Let G and H be groups.

Problem 3.1.1 Let $\varphi : G \to H$ be a homomorphism and let E be a subgroup of H. Prove that $\varphi^{-1}(E) \leq G$. If $E \trianglelefteq H$ prove that $\varphi^{-1}(E) \trianglelefteq G$. Deduce that $\ker \varphi \trianglelefteq G$.

Let $a, b \in \varphi^{-1}(E)$. Then we have that $\varphi(a), \varphi(b) \in E$. Since E is a subgroup, we have $\varphi(b)^{-1} \in E$ by inverses and $\varphi(a)\varphi(b)^{-1} \in E$ by closure. By the homomorphism property, we have $\varphi(ab^{-1}) \in E$, so $ab^{-1} \in \varphi^{-1}(E)$. Therefore, since $\varphi^{-1}(E) \neq \varnothing$, we have $\varphi^{-1}(E) \leq E$.

Now suppose $E \trianglelefteq H$. Let $g \in G$ and $a \in \varphi^{-1}(E)$. It suffices to show that $gag^{-1} \in \varphi^{-1}(E)$. Since E is normal, and $\varphi(a) \in E$, we have that

$$\varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g)^{-1} \in E,$$

so $gag^{-1} \in \varphi^{-1}(E)$ as desired.

Clearly, $\{e_H\} \trianglelefteq H$, and since $\ker \varphi = \varphi^{-1}(\{e_H\})$, it follows directly that $\ker \varphi \trianglelefteq G$. $\square$

Problem 3.1.2 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 let Y be the fiber above b, i.e., $X = \varphi^{-1}(a)$, $Y = \varphi^{-1}(b)$. Fix an element u of X (so $\varphi(u) = a$). Prove that if $XY = Z$ in the quotient group G/K and w is any member of Z, then there is some $v \in Y$ such that $uv = w$.

Let $w \in Z$. Then $\varphi(w) = ab$. Consider $v = u^{-1}w$. Then we have

$$\varphi(v) = \varphi(u^{-1}w) = \varphi(u)^{-1}\varphi(w) = a^{-1}ab = b,$$

so $v \in Y$. Thus, since $uv = uu^{-1}w = w$, the claim holds. $\square$

Problem 3.1.3 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.

Let $u, v \in G$. Then, we have

$$uN \cdot vN = (uv)N = (vu)N = vN \cdot uN,$$

so G/N is abelian.

An example is $G = S_3$, $N = A_3$. It is known that S_3 is not abelian and that A_3 is a normal subgroup. Let $\sigma, \tau \in S_3$. Then there are $m, n \in \mathbb{N}$ such that σ can be composed of m transpositions and τ can be composed of n transpositions. So both $\sigma\tau$ and $\tau\sigma$ can be composed of $m + n$ transpositions, so $(\sigma\tau)N = (\tau\sigma)N$. $\square$

Problem 3.1.4 Prove that in the quotient group G/N, $(gN)^\alpha = g^\alpha N$ for all $\alpha \in \mathbb{Z}$.

We have $(gN)^1 = g^1N$ trivially. It follows quickly from induction that $(gN)^n = g^nN$ for all $n \in \mathbb{Z}^+$, since $g^{n-1}NgN = g^nN$ by definition.

Also, we have $(gN)^0 = N = eN = g^0N$, since N is the identity in the factor group.

Finally, we have that $(gN)^{-1}$ is the inverse of gN in the factor group. We have that

$$(gN)(g^{-1}N) = (gg^{-1})N = eN = N$$

and

$$(g^{-1}N)(gN) = (g^{-1}g)N = eN = N,$$

so $g^{-1}N$ is the inverse of gN. Thus, $(gN)^{-1} = g^{-1}N$. It then follows from the result for positive α that for all $n \in \mathbb{Z}^-$, we have

$$(gN)^n = \left((gN)^{-n}\right)^{-1} = \left(g^{-n}N\right)^{-1} = (g^{-n})^{-1}N = g^nN.$$

□

Problem 3.1.5 Use Problem 3.1.4 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.

Let n be the smallest positive integer such that $g^n \in \mathbb{N}$. Then $(gN)^n = g^nN$ by Problem 3.1.4, and we have that $g^n \in \mathbb{N} \implies g^nN = N$. So $|gN| \leq n$. Now let $n' = |gN|$. So $(gN)^{n'} = N$, and we have $g^{n'}N = N$. So $g^{n'} \in N$, and thus $n' \geq n$ since n is the smallest positive integer such that $g^n \in \mathbb{N}$. So $|gN| = n$.

Consider $G = S_3$ and $N = A_3$. Then $g = (1\,2\,3)$ has order 3 in G, but gN has order 1 because $(1\,2\,3) \in A_3$, so $gN = N$. □

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

Let $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$. Then, we have

$$\begin{aligned}
\pi\left((x_1, y_1)\right) + \pi\left((x_2, y_2)\right) &= (x_1 + y_1) + (x_2 + y_2) \\
&= (x_1 + x_2) + (y_1 + y_2) \\
&= \pi\left((x_1 + x_2, y_1 + y_2)\right) \\
&= \pi\left((x_1, y_1) + (x_2, y_2)\right),
\end{aligned}$$

so π is a homomorphism. It is clearly surjective since for all $x \in \mathbb{R}$, $\pi\left((x, 0)\right) = x + 0 = x$.

The kernel of π is the set of points (x, y) in $\mathbb{R}^2$ such that $\pi\left((x, y)\right) = 0$. Thus, it is the set of points satisfying $x+y = 0$, that is, the line $y = -x$. The fiber of π above $a \in \mathbb{R}$ is likewise the set of points satisfying $x+y = a$, so the fiber above a is the line $y = -x + a$. □

Problem 3.1.9 Define $\varphi : C^\times \to \mathbb{R}^\times$ 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 $a + bi, c + di \in \mathbb{C}^\times$. Then we have

$$\begin{aligned}
\varphi(a + bi)\varphi(c + di) &= (a^2 + b^2)(c^2 + d^2) \\
&= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\
&= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 \\
&= (ac - bd)^2 + (ad + bc)^2
\end{aligned}$$

$$\begin{aligned}
&= \varphi\left((ac-bd)+(ad+bc)i\right) \\
&= \varphi\left(ac+adi+bci-bd\right) \\
&= \varphi\left((a+bi)(c+di)\right).
\end{aligned}$$

The image of φ is the positive real numbers: the sum of squares will always be positive since one of a or b will be non-zero, and for any $a \in \mathbb{R}^+$, we have $\varphi(\sqrt{a}) = a$.

The kernel of φ is the circle in the complex plane with radius 1. For any $a \in \mathbb{R}^+$, the fiber of φ above a is the circle in the complex plane with radius $\sqrt{a}$. □

Problem 3.1.10 Let $\varphi : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ by $\varphi(\overline{a}) = \overline{a}$. Show that this 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).

We first show that φ is well defined. Let $a, b \in \mathbb{Z}$ such that $\overline{a} = \overline{b}$ in $\mathbb{Z}/8\mathbb{Z}$: that is, $a \equiv b \pmod 8$ and thus there exists k so that $a - b = 8k$. Then for any $\alpha \in \varphi(\overline{a})$ and any $\beta \in \varphi(\overline{b})$, for some $m, n \in \mathbb{Z}$ we have

$$\begin{aligned}
\alpha - \beta &= (a+8m)-(b+8n) \\
&= a-b+8m-8n \\
&= 8k+8m-8n \\
&= 8(k+m-n) \\
&= 4\left(2(k+m-n)\right)
\end{aligned}$$

so $4 \mid (\alpha-\beta)$ and thus $\alpha \equiv \beta \pmod 4$. Therefore, $\varphi(\overline{a}) = \varphi(\overline{b})$, so φ is well-defined.

It is clear that φ is surjective: for any $\overline{a} \in \mathbb{Z}/4\mathbb{Z}$, there is some $a \in \mathbb{Z}$ such that $\overline{a}$ in $\mathbb{Z}/4\mathbb{Z}$, and we have that $\varphi(\overline{a}) = \overline{a}$ (where the first $\overline{a}$ is in $\mathbb{Z}/8\mathbb{Z}$).

The kernel of φ is $\{\overline{0}, \overline{4}\} \subset \mathbb{Z}/8\mathbb{Z}$. For all $\overline{a} \in \mathbb{Z}/4\mathbb{Z}$, the fiber of φ above $\overline{a}$ in $\mathbb{Z}/4\mathbb{Z}$ is $\{\overline{a}, \overline{a+4}\} \subset \mathbb{Z}/8\mathbb{Z}$. □

Problem 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 $0 \le q < 1$.

(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 $\mathbb{R}/\mathbb{Z}$.

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

(a) Let $x + \mathbb{Z}$ be a coset of $\mathbb{Q}/\mathbb{Z}$. Then $x + \mathbb{Z} = \{\ldots, x-2, x-1, x, x+1, x+2, \ldots\}$. Since each of these elements is 1 away from each other, it is clear that one of these elements is in $[0, 1)$.

(b) Let $x + \mathbb{Z}$ be a coset of $\mathbb{Q}/\mathbb{Z}$, and let q be the element in $x + \mathbb{Z}$. Let $q = \frac{a}{b}$ with $a, b \in \mathbb{Z}$. Then $bq = a$, and since $a \in \mathbb{Z}$, we have $b(x+\mathbb{Z}) = 0 + \mathbb{Z}$. Thus, $|x + \mathbb{Z}| \le b$ and thus $x + \mathbb{Z}$ has finite order. Also, for any order n, we have that $\frac{1}{n} + \mathbb{Z}$ has order n, so there are elements of arbitrarily large order.

(c) The torsion subgroup of $\mathbb{R}/\mathbb{Z}$ is $\{H \in \mathbb{R}/\mathbb{Z} : |H| < \infty\}$. From a previous homework problem, since $\mathbb{R}/\mathbb{Z}$ is abelian we have that torsion subgroup exists. It is clear from (b) that $\mathbb{Q}/\mathbb{Z}$ is a subset of the torsion subgroup. For the other inclusion, let $x + \mathbb{Z}$ in the torsion subgroup. Then $|x + \mathbb{Z}| < \infty$, so there exists some $b \in \mathbb{Z}$ such that $b(x+\mathbb{Z}) = 0 + \mathbb{Z}$. So there is some $a \in \mathbb{Z}$ such that $bx = a$, and thus $x = \frac{a}{b}$. Thus, $x \in \mathbb{Q}$, so $x + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$. □

(d) We have that the multiplicative group of root of unity in $C^\times$ is $U := \{z \in C^\times : z^n = 1 \text{ for some } n \in \mathbb{Z}\}$. Let $\varphi : \mathbb{Q}/\mathbb{Z} \to U$ be defined by

$$\varphi\left(\frac{a}{b} + \mathbb{Z}\right) = e^{2a\pi i/b},$$

where it is assumed that $\frac{a}{b} \in [0, 1)$. We have that $e^{2a\pi i/b} \in U$ because

$$\left(e^{2a\pi i/b}\right)^b = e^{2a\pi i} = \left(e^{2\pi i}\right)^a = 1^a = 1.$$

Now, let $\overline{p}, \overline{q} \in \mathbb{Q}/\mathbb{Z}$ such that $p = \frac{a}{b}$, $q = \frac{c}{d}$ for $a, b, c, d \in \mathbb{Z}$. Then we can write

$$\begin{aligned}
\varphi\left(\frac{\overline{a}}{b} + \frac{\overline{c}}{d}\right) &= \varphi\left(\overline{\frac{ad+bc}{bd}}\right) \\
&= e^{\frac{2(ad+bc)\pi i}{bd}} \\
&= e^{\frac{2ad\pi i}{bd} + \frac{2bc\pi i}{bd}} \\
&= \left(e^{\frac{2a\pi i}{b}}\right)\left(e^{\frac{2c\pi i}{d}}\right) \\
&= \varphi\left(\frac{\overline{a}}{b}\right)\varphi\left(\frac{\overline{c}}{d}\right),
\end{aligned}$$

so φ is a homomorphism.

Let $z = e^{i\theta} \in U$. Then $z^n = 1$ for some $n \in \mathbb{Z}$, so we have $n\theta i = 2\pi i$ and thus $n = 2\pi/\theta$. We observe that

$$\varphi\left(\frac{1}{n}\right) = e^{2\pi i/n} = e^{2\pi i\theta/2\pi} = e^{i\theta},$$

so φ is surjective.

Let $\frac{\overline{a}}{b}, \frac{\overline{c}}{d} \in \mathbb{Q}/\mathbb{Z}$ such that

$$\varphi\left(\frac{\overline{a}}{b}\right) = \varphi\left(\frac{\overline{c}}{d}\right).$$

Then we have

$$\begin{aligned}
&\varphi\left(\frac{\overline{a}}{b}\right) = \varphi\left(\frac{\overline{c}}{d}\right) \\
\implies &e^{\frac{2a\pi i}{b}} = e^{\frac{2c\pi i}{d}} \\
\implies &\frac{2a\pi i}{b} = \frac{2c\pi i}{d} \\
\implies &\frac{a}{b} = \frac{c}{d},
\end{aligned}$$

so φ is injective.

Therefore, φ is an isomorphism. $\square$

Problem 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 $[x, y]$.

($\Rightarrow$) Suppose $\overline{x}$ and $\overline{y}$ commute in $\overline{G}$. Then $(xy)N = (xN)(yN) = (yN)(xN) = (yx)N$. Thus, we have

$$\begin{aligned}
&(xy)N = (yx)N \\
\implies &\big((yx)N\big)^{-1}\big((xy)N\big) = \big((yx)N\big)^{-1}\big((yx)N\big)
\end{aligned}$$

$$\begin{aligned} \implies N &= \big((yx)N\big)^{-1}\big((xy)N\big) && (N \text{ is the identity of } G/N) \\ &= \Big((yx)^{-1}N\Big)\big((xy)N\big) && ((aH)^{-1} = a^{-1}H) \\ &= \Big(x^{-1}y^{-1}N\Big)\big((xy)N\big) \\ &= (x^{-1}y^{-1}xy)N, \end{aligned}$$

so $x^{-1}y^{-1}xy \in N$.

($\Leftarrow$) Suppose $x^{-1}y^{-1}xy \in N$. Then we have

$$\begin{aligned} & x^{-1}y^{-1}xy \in N \\ \implies & xx^{-1}y^{-1}xy \in xN \\ \implies & y^{-1}xy \in xN \\ \implies & yy^{-1}xy \in y(xN) \\ \implies & xy \in (yx)N \\ \implies & (xy)N = (yx)N \\ \implies & (xN)(yN) = (yN)(xN) \\ \implies & \overline{x} \cdot \overline{y} = \overline{y} \cdot \overline{x}, \end{aligned}$$

so $\overline{x}$ and $\overline{y}$ commute. □

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

Let $a \in G$ and $c \in N$. Then for some $m \in \mathbb{N}$ and some $x_1, \dots, x_m$, $y_1, \dots, y_m \in G$, we have

$$c = \prod_{i=1}^{m} x_i^{-1}y_i^{-1}x_iy_i.$$

Then, we can write

$$\begin{aligned} aca^{-1} &= a\prod_{i=1}^{m}\left(x_i^{-1}y_i^{-1}x_iy_i\right)a^{-1} \\ &= a\prod_{i=1}^{m}\left(x_i^{-1}a^{-1}ay_i^{-1}a^{-1}ax_ia^{-1}ay_i\right)a^{-1} \\ &= \prod_{i=1}^{m}\left(ax_i^{-1}a^{-1}\right)\left(ay_i^{-1}a^{-1}\right)\left(ax_ia^{-1}\right)\left(ay_ia^{-1}\right) \\ &= \prod_{i=1}^{m}\left(ax_ia^{-1}\right)^{-1}\left(ay_ia^{-1}\right)^{-1}\left(ax_ia^{-1}\right)\left(ay_ia^{-1}\right), \end{aligned}$$

so aca^{-1} is the product of commutators and thus $aca^{-1} \in N$. Therefore, $N \trianglelefteq G$. □

Let $a, b \in G$. We have $a^{-1}b^{-1}ab \in N$, so we can write

$$\begin{aligned} & a^{-1}b^{-1}ab \in N \\ \implies & \left(a^{-1}b^{-1}ab\right)N = N \\ \implies & \left((ba)^{-1}ab\right)N = N \end{aligned}$$

$$\begin{aligned}
&\implies \left((ba)^{-1}N\right)\left((ab)N\right) = N \\
&\implies \left((ba)N\right)^{-1}(ab)N = N \\
&\implies (ab)N = (ba)N \\
&\implies (aN)(bN) = (bN)(aN).
\end{aligned}$$

Therefore, G/N is abelian. □

Problem 3.1.42 Assume both H and K are normal subgroups of G with $H \cap K = \{1\}$. Prove that $xy = yx$ for all $x \in H$ and $y \in K$.

Let $x \in H$ and $y \in K$. Since H is normal, we have that $y^{-1}xy \in H$ since $y^{-1} \in G$ and $x \in H$, and by closure we have $x^{-1}\left(y^{-1}xy\right) \in H$. Since K is normal, we have that $x^{-1}y^{-1}x \in K$ since $x^{-1} \in G$ and $y^{-1} \in K$, and by closure we have $\left(x^{-1}y^{-1}x\right)y \in K$. So we have that $x^{-1}y^{-1}xy \in H \cap K$, and thus $x^{-1}y^{-1}xy = 1$ since $H \cap K = \{1\}$. Therefore, $xy = yx$. □

Problem 3.2.5 Let H be a subgroup of G and fix some element $g \in G$.

(a) Prove that gHg^{-1} is a subgroup of G of the same order as H.

(b) Deduce that if $n \in \mathbb{Z}^+$ and H is the unique subgroup of G of order n then $H \trianglelefteq G$.

(a) Consider $\varphi : H \to gHg^{-1}$ given by $\varphi(h) = ghg^{-1}$ for all $h \in H$. Then for all $h_1, h_2 \in H$ we have

$$\varphi(h_1h_2) = gh_1h_2g^{-1} = gh_1g^{-1}gh_2g^{-1} = \varphi(h_1)\varphi(h_2),$$

so φ is a homomorphism. Clearly, φ is surjective since for any $x \in gHg^{-1}$, we have $x = ghg^{-1}$ for some $h \in H$ and $\varphi(h) = x$. Also, φ is injective since for any $h_1, h_2 \in H$ with $\varphi(h_1) = \varphi(h_2)$, we have

$$gh_1g^{-1} = gh_2g^{-1} \implies gh_1 = gh_2 \implies h_1 = h_2.$$

So we can conclude that $H \cong gHg^{-1}$ via φ. Since we have $\varphi(H) = gHg^{-1}$ and φ is a homomorphism, gHg^{-1} is a subgroup of G since $gHg^{-1} \subseteq G$. Also, since φ is a bijection, we have $|H| = |gHg^{-1}|$.

(b) If H is the unique group of G of order n, then from part (a) we have $H = gHg^{-1}$ since $|H| = |gHg^{-1}|$. Thus, $H \trianglelefteq G$ by definition.

Problem 3.2.8 Prove that if H and K are finite subgroups of G whose orders are relatively prime then $H \cap K = \{1\}$.

We have that $H \cap K$ is a subgroup of both H and K, we have $|H \cap K| \,\Big|\, |H|$ and $|H \cap K| \,\Big|\, |K|$. Since $|H|$ and $|K|$ are relatively prime, their greatest common divisor is 1, so we have $|H \cap K| = 1$. Since every group has the identity, we must have $H \cap K = \{1\}$. □

Problem 3.2.10 Suppose H and K are subgroups of finite index in G with $|G : H| = m$ and $|G : K| = n$. Prove that $\text{lcm}(m, n) \le |G : H \cap K| \le mn$. Deduce that if m and n are relatively prime then $|G : H \cap K| = |G : H| \cdot |G : K|$.

Since $H \cap K$ is a subgroup of H and of K, we have from Problem 3.2.11 that

$$|G : H \cap K| = |G : H| \cdot |H : H \cap K| = m|H : H \cap K|$$

and

$$|G : H \cap K| = |G : K| \cdot |K : H \cap K| = n|H : H \cap K|.$$

Thus, we have that $|G : H \cap K|$ is a common multiple of m and n, so $\operatorname{lcm}(m, n) \leq |G : H \cap K|$. $\square$

For any left coset of $H \cap K$, we have

$$\begin{aligned} g(H \cap K) &= \{gx \mid x \in H \cap K\} \\ &= \{gx \mid x \in H \text{ and } x \in K\} \\ &= \{gx \mid x \in H\} \cap \{gx \mid x \in K\} \\ &= gH \cap gK. \end{aligned}$$

There are m left cosets of H and n left cosets of K, so there are at most mn left cosets of $H \cap K$ since for any $g(H \cap K) = gH \cap gK$, there are m choices for gH and n choices for gK. So $|G : H \cap K| \leq mn$.

It is known that $\gcd(m, n) \operatorname{lcm}(m, n) = mn$. If m and n are relatively prime, we have $\gcd(m, n) = 1$, so $\operatorname{lcm}(m, n) = mn$. Thus, we have $mn = \operatorname{lcm}(m, n) \leq |G : H \cap K| \leq mn$, so $|G : H \cap K| = mn$. $\square$

Problem 3.2.11 Let $H \leq K \leq G$. Prove that $|G : H| = |G : K| \cdot |K : H|$.

Let $\{g_i\}_{i \in I}$ be a set of representatives for $\{gK \mid g \in G\}$ and $\{k_j\}_{j \in J}$ be a set of representatives for $\{kH \mid k \in K\}$. Then define $\varphi : \{g_i\} \times \{k_j\} \to \{gH \mid g \in G\}$ by $\varphi\big((g, k)\big) = (gk)H$.

We claim that φ is a bijection. First, let $g \in G$. Since the left cosets of K partition G, we have that $g \in g_r K$ for some $g_r \in \{g_i\}$, so $= g_r k$ for some $k \in K$. Since the left cosets of H partition K, we have that $k \in k_r H$ for some $k_r \in \{k_j\}$, so $k = k_r h$ for some $h \in H$. Thus, we have $g = g_r k_r h$, so $g \in (g_r k_r)H$. Then we have

$$\varphi\big((g_r, k_r)\big) = (g_r k_r)H = gH,$$

so φ is surjective.

Now, let $g, g' \in \{g_i\}$ and $k, k' \in \{k_j\}$ such that $\varphi\big((g, k)\big) = \varphi\big((g', k')\big)$. Then, $(gk)H = (g'k')H$. Note that $kH \subseteq K$ and $k'H \subseteq K$ since $H \leq K$. Then, if $g \neq g'$, we would have $gK \cap g'K = \varnothing$ and thus $g(kH) \cap g'(k'H) = \varnothing$, contradicting

$$g(kH) = (gk)H = (g'k')H = g'(k'H).$$

So we have $g = g'$, and thus $kH = k'H$, which implies $k = k'$. So φ is injective.

Since φ is a bijection, we then have

$$|G : H| = |\{gH | g \in G\}| = |\{g_j\} \times \{k_i\}| = |\{g_i\}| \cdot |\{k_j\}| = |G : K| \cdot |K : H|.$$

$\square$

Problem 3.2.16 Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ to prove Fermat's Little Theorem: if p is a prime then $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{Z}$.

We have that $(\mathbb{Z}/p\mathbb{Z})^\times$ has order $p-1$. For any $a \in \mathbb{Z}$, we have that the order of $\overline{a}$ divides $p-1$ by Lagrange's theorem, so there exists $k \in \mathbb{Z}$ such that $|\overline{a}|k = p - 1$. So we have

$$a^p = a \cdot a^{p-1} = a \cdot a^{|\overline{a}|k} = a \cdot \left(a^{|\overline{a}|}\right)^k \equiv a \cdot 1^k = a \pmod{p}.$$

$\square$

Problem 3.2.18 Let G be a finite group, let H be a subgroup of G and let $N \trianglelefteq G$. Prove that if $|H|$ and $|G : N|$ are relatively prime then $H \leq N$.

Let $\pi : G \to G/N$ be defined by $\pi(g) = gN$. Then, since π is clearly a homomorphism, we have $\pi(H) \leq G/N$, so $|\pi(H)|$ divides $|G : N|$ by Lagrange's theorem. For $\pi|_H : H \to G/N$, we have $\ker \varphi = H \cap N$. Thus, from the First Isomorphism Theorem we have $H/(H \cap N) \cong \pi(H)$, so $|\pi(H)|$ divides $|H|$. So $|\pi(H)| = 1$, so $\pi(H) \leq \ker(\varphi) = N$. □

Problem 3.2.22 Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ to prove Euler's Theorem: $a^{\varphi(n)} \equiv 1 \pmod{n}$ for every integer a relatively prime to n, where φ denotes Euler's φ-function.

We have that $(\mathbb{Z}/n\mathbb{Z})^\times$ has order $\varphi(n)$. For any $a \in \mathbb{Z}$, we have that the order of $\overline{a}$ divides $\varphi(n)$ by Lagrange's theorem, so there exists $k \in \mathbb{Z}$ such that $|\overline{a}|k = \varphi(n)$. So we have

$$a^{\varphi(n)} = a^{|\overline{a}|k} = \left(a^{|\overline{a}|}\right)^k \equiv 1^k = 1 \pmod{n}.$$

□

Problem 3.2.23 Determine the last two digits of $3^{3^{100}}$.

We have that $\varphi(40) = 16$, so from Problem 3.2.22 we have $3^{16} \equiv 1 \pmod{40}$. Again applying Problem 3.2.22 we have

$$3^{100} = 3^4 \cdot \left(3^{16}\right)^6 \equiv 3^4 \cdot 1^6 = 3^4 = 81 \equiv 1 \pmod{40}.$$

So there exists k such that $40k = 3^{100} - 1$.

We have that $\varphi(100) = 40$, so from Problem 3.2.22 we have $3^{40} \equiv 1 \pmod{100}$. So we can write

$$3^{3^{100}} = 3^1 \cdot 3^{3^{100}-1} = 3^1 \cdot 3^{40k} = 3^1 \cdot \left(3^{40}\right)^k \equiv 3^1 \cdot 1^k = 3 \pmod{100}.$$

So the last two digits of $3^{3^{100}}$ are 03. □