# Elements of solution for Homework 5

## General remarks

### How to use the First Isomorphism Theorem

A standard way to prove statements of the form '$G/H$ *is isomorphic to* $\Gamma$' is to construct a homomorphism $\varphi : G \longrightarrow \Gamma$ such that

1. $\varphi$ is surjective (that is $\operatorname{Im}\varphi = \Gamma$)
2. $\ker\varphi = H$.

Then, the Isomorphism Theorem states that there exists an isomorphism[1] between $G/\ker\varphi = G/H$ and $\operatorname{Im}\varphi = \Gamma$

### Left and right cosets

A subgroup $H$ of a group $G$ is normal if $ghg^{-1} \in H$ for every $g \in G$ and $h \in H$. This condition can be rephrased as

$$gHg^{-1} = H$$

which in turn is equivalent to having $gH = Hg$ for every $g \in G$. In other words, if $H \triangleleft G$, then for every $g \in G$ and every $h \in H$, there exist $h'$ and $h''$ in $H$ such that

$$gh = h'g \qquad \text{and} \qquad hg = gh''.$$

### Neutral element in a quotient

If $H$ is a normal subgroup of a group $G$, the neutral element of $G/H$ is the class modulo $H$ of the neutral element of $G$:

$$e_{G/H} = [e_G] = e_G H = \{e_G h\ ,\ h \in H\} = H.$$

[1] Namely the homomorphism $\tilde{\varphi}$ induced by $\varphi$ and defined by $\tilde{\varphi}(gH) = \varphi(g)$.

# Chapter 15

## A.1

For $n \in \mathbb{Z}$, we denote by $[n]$ the class of $n$ modulo 10[2]. Then, with

$$H = \{[0], [5]\} < \mathbb{Z}/10\mathbb{Z},$$

the cosets are of the form

$$\bar{n} := [n] + H = \{[n], [n] + [5]\} = \{[n], [n+5]\}.$$

So a list of the elements in $G/H$ is

$$\bar{0} = \bar{5} \quad , \quad \bar{1} = \bar{6} \quad , \quad \bar{2} = \bar{7} \quad , \quad \bar{3} = \bar{8} \quad , \quad \bar{4} = \bar{9}.$$

To prove that $G/H$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$, a concrete way is to verify that the map sending $\bar{n}$ to the class of $n$ modulo 5 is an isomorphism. An abstract way is to recall that if $p$ is prime (e.g. $p = 5$), all groups of order $p$ are isomorphic (and cyclic ).

## A.2

Observe that $H = \{\mathrm{Id}, (1\,2\,3), (1\,3\,2)\}$ is the alternating subgroup $\mathfrak{A}_3$ of $G = \mathfrak{S}_3$.

Since $|G| = 6$ and $|H| = 3$, Lagrange's Theorem predicts that the number of classes is

$$[G : H] = \frac{|G|}{|H|} = 2.$$

One class has to be $\mathrm{Id}H = H$, neutral element of $G/H$ and the other has to be the complement, namely $T = \{(1\,2), (1\,3), (2\,3)\}$. This group is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

## A.5

The subgroup $H$ generated by $(0, 1)$ in $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has two elements: $(0, 1)$ and $(0, 1) + (0, 1) = (0, 0)$.

Therefore, if $(a, b) \in G$, its class modulo $H$ consists of $(a, b)$ and $(a, b + 1)$. There are four such classes, determined by the value of $a$.

[2] A representative of this class is the last digit of $n$.

There exist two non-isomorphic groups of order $4$, namely $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$[3]. To see that $G/H$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$, one can either write down the table or observe that the map

$$\begin{array}{ccc} G & \longrightarrow & \mathbb{Z}/4\mathbb{Z} \\ (a,b) & \longmapsto & a \end{array}$$

is a surjective homomorphism with kernel $H$ and apply the isomorphism Theorem.

**Notation:** in all subsequent problems, the class of an element $x \in G$ in a quotient $G/H$ will be denoted by $[x]$.

## C.1

Let $H$ be a subgroup of a group $G$. Assume that $x^2 \in H$ for every $x \in G$ and let $A$ be an element of $G/H$. Then if $a$ is a representative of $A$ in $G$, that is, $A = [a]$, we have

$$A \cdot A = [a] \cdot [a] = [a^2] = H = e_{G/H}$$

which exactly means that $A$ is its own inverse.

Conversely, assume that every element of $G/H$ is its own inverse. It follows that $[x] \cdot [x] = e_{G/H}$ for every $x \in G$. In other words, $[x^2] = H$ which exactly means that $x^2 \in H$ for every element $x \in G$.

## C.5

Let $H$ be a subgroup of a group $G$. Assume that $G/H$ is cyclic. This means that there exists and element $A \in G/H$ such that $G/H = \langle A \rangle$. In other words, every element $X \in G/H$ is of the form $A^n$ with $n \in \mathbb{Z}$.

Therefore, if $a$ is a representative of $A$ in $G$ and $x$ is any element of $G$, there exists an integer $n_0 \in \mathbb{Z}$ such that

$$[x] = [a]^{n_0} = [a^{n_0}].$$

This exactly means that $x$ and $a^{n_0}$ are equivalent modulo $H$, which translates as $xa^{-n_0} \in H$. Let $n = -n_0$ to recover the statement expected in the book.

Conversely, assume the existence of an element $a$ in $G$ such that for every element $x \in G$, there exists an integer $n$ such that $xa^n \in H$.
For $X \in G/H$, let $x$ be a representative of $X$. Then the hypothesis implies that

$$X \cdot [a]^n = [x] \cdot [a]^n = [xa^n] = H = e_{G/H}.$$

It follows that $X = [a^{-1}]^n$ so $[a^{-1}]$ generates $G/H$, which is therefore cyclic[4].

[3]This group, in which every element has order 2, is called Klein's group and denoted by $V_4$.

[4]Note that $[a]$ and $[a^{-1}] = [a]^{-1}$ generate the same subgroup of $G/H$.

## F.1 to F.4

Let $G$ be a group and $C$ its center. Recall that $C \triangleleft G$ in general and assume that $G/C$ is cyclic, generated for instance by $A \in G/C$.

As in **C.5**, if $x \in G$ and $a$ is a representative of $A$ in $G$, there exists an integer $m$ such that $[x] = [a]^m$ which implies that the equality of cosets

$$Cx = Ca^m.$$

A reformulation of this is the fact that $x$ and $a^m$ are equivalent modulo $C$, that is, $x(a^m)^{-1} \in C$, which is equivalent to the existence of $c \in C$ such that $x(a^m)^{-1} = c$, or

$$x = ca^m.$$

To prove that $G$ is abelian, let $x$ and $y$ be elements of $G$. It follows from what we just did that

$$x = ca^m \qquad \text{and} \qquad y = c'a^{m'}$$

for some $c, c' \in C$ and $m, m' \in \mathbb{Z}$. Then,

$$\begin{array}{rcll} xx' & = & ca^m c'a^{m'} & \\ & = & c'(ca^m)a^{m'} & \text{because } c' \in C \\ & = & c'ca^{m+m'} = c'ca^{m'}a^m & \text{by associativity} \\ & = & c'a^{m'}ca^m & \text{because } c \in C \\ & = & x'x, & \end{array}$$

which shows that the multiplication in $G$ is commutative.

# Chapter 16

## A.3

With the notation of Problem **A.2** in Chapter 15, we want to verify that $\mathfrak{S}_3/\mathfrak{A}_3$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. The method actually works for $\mathfrak{S}_n/\mathfrak{A}_n$ with $n$ arbitrary.

Consider the signature homomorphism

$$\varepsilon : \mathfrak{S}_n \longrightarrow (\{-1, 1\}, \times)$$

the isomorphism

$$\begin{array}{rcl} \iota : (\{-1,1\}, \times) & \longrightarrow & (\mathbb{Z}/2\mathbb{Z}, +) \\ 1 & \longmapsto & 0 \\ -1 & \longmapsto & 1 \end{array} .$$

The composition

$$\iota \circ \varepsilon : \mathfrak{S}_n \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

maps even permutations to $0$ and odd permutations to $1$. It is a surjective homomorphism with kernel $\mathfrak{A}_n$. The result then follows from the First Isomorphism Theorem.

## A.5

Let $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $H$ the diagonal subgroup $\{(a, a), a \in \mathbb{Z}/3\mathbb{Z}\}$. As suggested, consider the map

$$\begin{array}{rccc} f: & G & \longrightarrow & \mathbb{Z}/3\mathbb{Z} \\ & (a,b) & \longmapsto & a-b \end{array}.$$

For any $a, b, a', b' \in \mathbb{Z}/3\mathbb{Z}$,

$$\begin{aligned} f((a,b)+(a',b')) &= f(a+a', b+b') \\ &= a + a' - (b + b') \\ &= a - b + a' - b' \\ &= f((a,b)) + f((a',b')) \end{aligned}$$

so $f$ is a homomorphism. It is surjective since every $a \in \mathbb{Z}/3\mathbb{Z}$ is the image under $f$ of the couple $(a, 0)$. In addition, the kernel of $f$ is the set of couples $(a, b)$ such that $a - b = 0$, which is exactly $H$. Therefore, by the First Isomorphism Theorem, $f$ induces an isomorphism from $G/H$ to $\mathbb{Z}/3\mathbb{Z}$.

## D

Let $G$ be a group. By $\mathrm{Aut}(G)$, we mean the set of isomorphisms from $G$ to itself, that is the set of bijective homomorphisms (*automorphisms*) from $G$ to itself:

$$\mathrm{Aut}(G) = \mathrm{Hom}(G, G) \cap \mathrm{Bij}(G).$$

Automorphisms form by definition a subset of the group $(\mathrm{Bij}(G), \circ)$. We shall prove that $\mathrm{Aut}(G)$ is in fact a subgroup of $\mathrm{Bij}(G)$. Note that the the map $\mathrm{Id} : g \longmapsto g$ is an automorphism so that $\mathrm{Aut}(G)$ is not empty.
Let $u, v \in \mathrm{Aut}(G)$. Then $u \circ v$ is bijective as a composition of bijections. To verify that that $u \circ v$ is a homomorphism, let $g, g' \in G$. Then

$$\begin{aligned} u \circ v(gg') &= u(v(gg')) \\ &= u(v(g)v(g')) && \text{because } v \text{ is a homomorphism} \\ &= u(v(g))\, u(v(g')) && \text{because } u \text{ is a homomorphism} \\ &= u \circ v(g)\, u \circ v(g'). \end{aligned}$$

Finally, we prove that $\mathrm{Aut}(G)$ is stable under taking inverses. Every $u \in \mathrm{Aut}(G)$ has an inverse $u^{-1}$ in $\mathrm{Bij}(G)$. We want to prove that $u^{-1}$ is a homomorphism, that is

$$(\dagger) \qquad u^{-1}(gg') = u^{-1}(g)u^{-1}(g')$$

for every $g, g' \in G$. By definition of inverse maps, $u^{-1}(gg')$ is the *unique* element of $G$ that is mapped to $gg'$ by $u$. Therefore, to prove $(\dagger)$, it suffices to prove that the image of the right-hand side by $u$ is $gg'$. Since $u$ is a homomorphism, we get

$$u\left(u^{-1}(g)u^{-1}(g')\right) = \underbrace{u\left(u^{-1}(g)\right)}_{=g}\underbrace{u\left(u^{-1}(g')\right)}_{=g'}$$

hence the result.

Let us fix an element $a$ in $G$. Then, the associated conjugation map

$$\begin{array}{rcl} \varphi_a : G & \longrightarrow & G \\ g & \longmapsto & aga^{-1} \end{array}$$

is an automorphism:

- for $g, g' \in G$,

$$\varphi_a(gg') = agg'a^{-1} = ag\underbrace{a^{-1}a}_{=e_G}g'a^{-1} - = \varphi_a(g)\varphi_a(g').$$

- Injectivity:
$$\varphi_a(g) = e_G \Leftrightarrow aga^{-1} = e_G \Leftrightarrow g = a^{-1}e_Ga = e_G$$
so $\ker \varphi_a = \{e_G\}$.
- Surjectivity: for $h \in G$,

$$\varphi_a(a^{-1}ha) = aa^{-1}haa^{-1} = h.$$

**N.B.** The proof of surjectivity also shows that $(\varphi_a)^{-1} = \varphi_{a^{-1}}$.

Automorphisms of the form $\varphi_a$ are called *inner*. We shall prove that the set $\mathrm{Inn}(G)$ of inner automorphisms is a subgroup of $\mathrm{Aut}(G)$. We know that the image of a group homomorphism is a subgroup of the target group, so it suffices to prove that the map

$$\begin{array}{rcl} h : G & \longrightarrow & \mathrm{Aut}(G) \\ a & \longmapsto & \varphi_a \end{array}$$

is a group homomorphism to get $\mathrm{Inn}(G) = \mathrm{Im}\, h < \mathrm{Aut}(G)$.

Let $a, b \in G$. For every $g \in G$,

$$\begin{aligned} h(ab)(g) &= \varphi_{ab}(g) \\ &= (ab)g(ab)^{-1} \\ &= abgb^{-1}a^{-1} \\ &= a\varphi_b(g)a^{-1} \\ &= \varphi_a\left(\varphi_b(g)\right) \\ &= \varphi_a \circ \varphi_b(g) \\ &= h(a) \circ h(b)(g). \end{aligned}$$

Therefore $h(ab) = h(a) \circ h(b)$ and $h \in \mathrm{Hom}(G, \mathrm{Aut}(G))$.

Since $\mathrm{Inn}(G) = \mathrm{Im}\, h$ by definition, the First Isomorphism Theorem implies that $\mathrm{Inn}(G)$ is isomorphic to $G/\ker h$.

The kernel of $h$ is the set of elements $a \in G$ such that $\varphi_a = \mathrm{Id}$, that is, the elements $a$ such that $aga^{-1} = g$ for all $g \in G$. Left multiplying by $a^{-1}$, we see that $a$ is in $\ker h$ if and only if $a$ is in the center $\mathcal{Z}(G)$ of $G$.

As a conclusion,

$$\mathrm{Aut}(G) > \mathrm{Inn}(G) \simeq G/\mathcal{Z}(G).$$