HW 2

Ravi Kini

October 17, 2023

Problem 1

Let $a, b \in G$. Since $a^{-1}(ab)a = \left(a^{-1}a\right)(ba) = ba$, ba is the conjugate of ab by a^{-1}. We now show that $a^{-1}(ab)^k a = (ba)^k$. The case where $k = 1$ was shown above. Assume that this holds for some k. Then:

$$\begin{aligned} a^{-1}(ab)^{k+1}a &= a^{-1}(ab)^k(ab)a \\ &= a^{-1}(ab)^k a(ba) \\ &= (ba)^k(ba) = (ba)^{k+1} \end{aligned} \tag{1}$$

By the Principle of Mathematical Induction, $a^{-1}(ab)^k a = (ba)^k$ for all $k \in \mathbb{Z}$. Suppose ab is of infinite order. Then, for all $n \in \mathbb{N}$:

$$\begin{aligned} (ab)^n &\neq 1 \\ a^{-1}(ab)^n a &\neq a^{-1}a = 1 \\ (ba)^n &\neq 1 \end{aligned} \tag{2}$$

Therefore ba is also of infinite order. Now suppose ab is of finite order, with $n := \operatorname{ord}(ab)$:

$$\begin{aligned} (ab)^n &= 1 \\ a^{-1}(ab)^n a &= a^{-1}a = 1 \\ (ba)^n &= 1 \end{aligned} \tag{3}$$

Since $(ab)^n = 1 \iff (ba)^n = 1$, it is impossible for there to be some $n' < n$ such that $(ba)^{n'} = 1$, as that would imply $(ab)^{n'} = 1$, contradicting the definition of n. Therefore $\operatorname{ord}(ba) = n$, and $\operatorname{ord}(ab) = \operatorname{ord}(ba)$.

Problem 2

***Algebra* (Artin, 2e) Exercise 2.4.10**

Take the group of 2×2 matrices $G = GL_2(\mathbb{R})$. The matrices A, B are elements with order 2:

$$\begin{aligned} A &= \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \\ A^2 &= \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1_G \\ B &= \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \\ B^2 &= \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = 1_G \end{aligned} \tag{4}$$

However, their product AB is of infinite order, as there is no n such that $(AB)^n = 1_G$. We instead assert that $(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. In the case where $n = 1$:

$$AB = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \neq 1_G \tag{5}$$

Clearly the assertion holds for $n = 1$. Assume that this assertion holds for some n. Then:

$$\begin{aligned} (AB)^{n+1} &= (AB)^n (AB) \\ &= \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix} \neq 1_G \end{aligned} \tag{6}$$

By the Principle of Mathematical Induction, $(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \neq 1_G$ for all $n \in \mathbb{N}$. Consequently, $\operatorname{ord}(AB) = \infty$.

In the case of an abelian group, let G be some abelian group and $a, b \in G$ with $m := \operatorname{ord}(a), n := \operatorname{ord}(b)$. We assert that $(ab)^k = a^k b^k$. Clearly the assertion holds for $k = 1$, when $(ab)^1 = ab = a^1 b^1$. Assume that this assertion holds for some k. Then:

$$\begin{aligned} (ab)^{k+1} &= (ab)^k (ab) \\ &= \left(a^k b^k\right)(ab) = a^k \left(b^k a\right) b = a^k \left(ab^k\right) b \\ &= (a^n k)\left(b^k b\right) \\ &= a^{k+1} b^{k+1} \end{aligned} \tag{7}$$

By the Principle of Mathematical Induction, $(ab)^k = a^k b^k$ for all $k \in \mathbb{N}$. Let there be some $p \in \mathbb{Z}$ such that $m|p$ and $n|p$, or equivalently, $p = m \cdot i = n \cdot j$ for $i, j \in \mathbb{Z}$. Then:

$$\begin{aligned} (ab)^p &= a^p b^p \\ &= a^{m \cdot i} b^{n \cdot j} \\ &= (a^m)^i (b^n)^j \\ &= 1_G^i 1_G^j = 1_G 1_G = 1_G \end{aligned} \tag{8}$$

Since $(ab)^p = 1$, $p \in \{n \in \mathbb{N} \ : \ g^n = 1\}$, which means that $p \geq \min \{n \in \mathbb{N} \ : \ g^n = 1\}$. Since p is finite, $p < \infty$, and $\operatorname{ord}(ab) < \infty$, which means ab has finite order.

Problem 3

***Algebra* (Artin, 2e) Exercise 2.4.5**

Let $G = \langle g \rangle$ be some cyclic group of order n, and H a subgroup of G. If H is either the trivial subgroup or G, both subgroups are evidently cyclic. Suppose H is then a proper subgroup of G that is not the trivial subgroup. As G is $\left\{1, g, g^2, \ldots g^{n-1}\right\}$, H, being a subset of G must contain only integral powers of g as well. Let m be the least positive integer such that $g^m \in H$. Let some $g^p \in H$. By the division theorem, there exist $q, r \in \mathbb{Z}$ where $0 \leq r < m$ such that $p = mq + r$. Then:

$$\begin{aligned} g^m &\in H \\ (g^m)^q = g^{mq} &\in H \\ (g^{mq})^{-1} = g^{-mq} &\in H \\ g^p g^{-mq} = g^{p-mq} = g^r &\in H \end{aligned} \tag{9}$$

Since m is the least positive integer such that $g^m \in H$, $r = 0$. Consequently, every element of H can be represented as $g^p = g^{mq} = (g^m)^q$, which means H is the cyclic subgroup of G generated by g^m. In all cases, H is cyclic, which means that every subgroup of a cyclic group is cyclic.

Problem 4

***Algebra* (Artin, 2e) Exercise 2.5.3**

Let $A, B \in U$ such that:

$$A = \begin{bmatrix} a_A & b_A \\ 0 & d_A \end{bmatrix}, B = \begin{bmatrix} a_B & b_B \\ 0 & d_B \end{bmatrix} \tag{10}$$

Then:

$$\begin{aligned} AB &= \begin{bmatrix} a_A & b_A \\ 0 & d_A \end{bmatrix} \begin{bmatrix} a_B & b_B \\ 0 & d_B \end{bmatrix} = \begin{bmatrix} a_A a_B & a_A b_B + b_A d_B \\ 0 & d_B \end{bmatrix} \\ \phi(AB) &= (a_A a_B)^2 = a_A^2 a_B^2 = \phi(A) \times \phi(B) \end{aligned} \tag{11}$$

Therefore ϕ is a homomorphism.

The kernel of ϕ is $\{A \in U \ : \ \phi(A) = 1\}$. Then:

$$\begin{aligned} \phi(A) = a^2 &= 1 \\ a^2 - 1 = (a+1)(a-1) &= 0 \\ a &= \pm 1 \end{aligned} \tag{12}$$

Consequently, $\ker\phi = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \ : \ a \in \{\pm 1\}, \ b, d \in \mathbb{R}, \ ad \neq 0 \right\} \subset U$.

The image of ϕ is $\{r \in \mathbb{R} \ : \ \exists A \in G (\phi(A) = r)\}$. Since $r = a^2$ for $a \in \mathbb{R}$, $r \geq 0$. Furthermore, since $ad \neq 0$, $a \neq 0$, so $r > 0$. Consequently, $\mathrm{img}\phi = (0, \infty)$.

Problem 5

***Algebra* (Artin, 2e) Exercise 2.5.4**

Let $x, y \in \mathbb{R}$. Then:

$$\begin{aligned} f(x+y) &= e^{i(x+y)} \\ &= e^{ix+iy} \\ &= e^{ix}e^{iy} \\ &= f(x) \times f(y) \end{aligned} \tag{13}$$

Therefore f is a homomorphism.

The kernel of f is $\{x \in \mathbb{R} \ : \ f(x) = 1\}$. Then:

$$\begin{aligned} \phi(x) = e^{ix} &= \cos x + i \sin x = 1 \\ x &= 2\pi n \end{aligned} \tag{14}$$

Consequently, $\ker f = 2\pi n$ for $n \in \mathbb{Z}$.

The image of f is $\{z \in \mathbb{C} \ : \ \exists x \in \mathbb{R}\,(f(x) = z)\}$. Since $z = e^{ix}$ for $x \in \mathbb{R}$, we see that $|z| = |e^{ix}| = 1$. Consequently, $\mathrm{img} f = \{z \in C \ : \ |z| = 1\}$.