Euler Circle

Albert Ye

April 1, 2020

§1 Week 1

§1.1 Solutions

A few interesting problems I've done:

2) (needed for 20) We know that $gH(gh)^{-1} = e = geg^{-1} = ghh^{-1}g^{-1} = gh(h^{-1}g^{-1})$. So $(gh)^{-1} = h^{-1}g^{-1}$. ■

6) Let us start at a complex value z. $\rho\tau$ is adding x and taking the negative of the value $z + x$. $\tau\rho^{-1}$ is taking the negative of z and subtracting x. Both outcomes lead to $-z - x$. ■

8) By definition, μ_n is a root of unity. The rest follows trivially. ■

11) Translations and glide reflections cannot work because they move the point irreparably away from the origin. For rotations, any rotation across a center $\neq (0, 0)$ will bring the point out of the origin. The center must be $(0, 0)$ and the angle can be anything. For reflections, any line that does not intersect $(0, 0)$ will take the point out of the origin, so only lines going through $(0, 0)$ can work.

20) We can just let τ be τ because $\tau^2 = e$. For ρ, we note that any rotation is a composition of two non-parallel lines. Hence, ρ can be expressed as two reflections, each of which can be reversed in one step. ■

21) We know from (2) that $gh = (gh)^{-1} = h^{-1}g^{-1} = hg$. ■

22) Fix two elements a, b in G. Assume that $ab \neq ba$. Then there are at best 5 elements a, b, ab, ba, e. However, we are given that G is order 4, contradiction. ■

23) Every element must have an inverse by definition of group. Because G is a group, all of the elements not with order 2 have some other inverse in the group. Commutativity allows us to pair up each element with its inverse. Hence, all that remains are the ones who only have inverses as themselves because they were only counted once – the rest all turned into identity.

For Wilson's, substitute $\mathbb{Z}/p\mathbb{Z}$ as G with multiplication as the operation. $(p-1)!$ is the product of all numbers $1 \cdots p - 1$. Everything cancels out except for the ones with inverse as themself, namely 1 and $p - 1$. Hence, the residue is -1. ■

§2 Week 2

§2.1 Notes

§2.1.1 Subgroup

Definition 2.1. Let G be a group. A nonempty subset H of G is a **subgroup** of G if

- $h_1, h_2 \in H \implies h_1h_2 \in H$

- $h \in H \implies h^{-1} \in H$

If H is a subgroup of G we denote $H \leq G$.

Here is another way to create groups from groups:

§2.1.2 Direct Product

Definition 2.2. Let G, H be groups. Let their direct product $G \times H$ whose set is $\{(g,h) \forall g \in G, h \in H\}$ and whose operation is $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$.

§2.1.3 Homomorphism

Definition 2.3. Let G, H be groups. A **homomorphism** is a function $f : G \to H$ s.t. $f(g_1 g_2) = f(g_1) f(g_2)$.

Homomorphisms must *always* exist. Just see $f(g) = e_H \forall g \in G$.

Proposition 2.4

Let $f : G \to H$ be a homomorphism between groups G, H.

- $f(e_G) = e_H$
- $f(g^{-1}) = f(g)^{-1}$.
- order of $g \in G$ is $n \implies$ order of $f(g) \in H$ is *at most* n.

Proof. 1) $f(e_G) = f(e_G e_G) = f(e_G) f(e_G) \implies e_H = f(e_G)$
2) $e_H = f(e_G) = f(gg^{-1}) = f(g) f(g^{-1})$. Multiply by $f(g^{-1})$ to get the desired.
3) Let $g^n = e$. Then $e_H = f(e_G) = f(g^n) = f(g)^n$. This only shows that $f(g)$ has order $\leq n$. Just see the trivial homomorphism. □

Definition 2.5. Let $f : G \to H$ be a homomorphism.

- The **kernel** of f is the set of elements in G s.t. $f(g) = e_H$.
- The **image** of f is the set of elements in H that take on a value of $f(g)$ for some $g \in G$.

Definition 2.6. We call $f : X \to Y$:

- *injective* if $a = b \implies f(a) = f(b) \forall a, b \in X$.
- *surjective* if Y is the image of f.

Proposition 2.7

We claim that

- Kernels and images are subgroups.
- f is injective iff the kernel of f is $\{e_G\}$.
- Something else true by definition.

§2.1.4 Isomorphisms

Definition 2.8. An **isomorphism** is a bijective homomorphism.

Example: $f : \mathbb{R} \to (\mathbb{R}_{>0}, \times), f(x) = e^x$.

Definition 2.9. An **automorphism** is the isomorphism $f : G \to G$.

Definition 2.10. The **conjugate** of g by h is $hgh^{-1} \in G$. The **conjugacy class** is the set of all such conjugates.

§2.1.5 Group Actions

Groups should be looked at as movements.

Definition 2.11. Let X be a set, G a group. (X can be any set.) A **left action** of G on X is a function $f : G \times X \to X$ s.t.

- $ex = x \forall x \in X$
- $(g_1 g_2)x = g_1(g_2 x) \forall g_1, g_2 \in G, x \in X$

A **right action** is defined similarly.

Definition 2.12. Alternatively, each $g \in G$ gives a permutation of the elements of X, i.e. an element of S_X. A **group action** is a homomorphism $f : G \to S_X$.

Important:

- All groups act on themselves with left multiplication
- G acts on itself by conjugation on $G \times X : X$

Theorem 2.13

Any finite group is isomorphic to a subgroup of S_n for some positive integer n.

This looks nice, but is really inefficient. $|S_n|$ is literally factorial time!

To prevent collapsing elements into one x value, we define

Definition 2.14. A group action $G \to x$ is **faithful** if whenever $gx = x \forall x \in X$, then $g = e$.