PSET2

Student: Ryan Baldwin, `rbaldwi2@swarthmore.edu`
Lecturer: Dr. Hsu
Collaborators:
Peer Reviewers:
Due Date: February 7, 2025

Artin Section 2: 2.6

$\Diamond$ Let G be a group. Define an *opposite group* G° with law of composition $a * b = ba$. Prove that G° is a group.

Proof. Given that G° is composed of elements in the group G, we shall prove that the *opposite group* $(G^\circ, *)$ is indeed a group.

To begin, we shall demonstrate that G° has closure under its law of composition:$*$. We notice that since G is indeed a group with elements $a, b, ab, ba \in G$, G° would have the exact same elements as well.

These truths consequently prove that

$$a * b = ba \in G^\circ$$
$$b * a = ab \in G^\circ$$

Therefore, $(G^\circ, *)$ is closed under its law of composition.

Now notice that G° has the identity of G which we shall notate as 1. Given any element a, it can then be shown that

$$a * 1 = 1a = a1 * a = a1 = a$$

Showing that indeed the identity element is in G°.

Since G° is comprised of all the elements of group G, there must be a and a^{-1} in G° such that

$$a * a^{-1} = a^{-1}a = 1$$
$$a^{-1} * a = aa^{-1} = 1$$

Proving that G° does indeed have inverses for all elements in its set.

Lastly, consider three elements a, b and c in group G that are consequently all in G°. By the law of composition of $(G^\circ, *)$,

$$(a * b) * c = c(a * b) = c(ba)$$

Indeed, it can then be observed that the element $c(ba)$ can be algebraically manipulated to obtain

$$c(ba) = (cb)a = a * (cb) = a * (b * c)$$

Hence,

$$(a * b) * c = a * (b * c)$$

Indeed associativity has been proven to hold under G° and indeed we have sufficiently proven that G° is a group. $\square$

Artin Section 4: 4.1

$\Diamond$ Let a and b be elements of a group G. Assume that a has order 7 and that $a^3b = ba^3$. Prove that $ab = ba$.

Proof. We shall prove directly that the group G with a multiplicative law of composition is abelian with the provided relation $a^3b = ba^3$ and that a has order 7.

Assume that $ab = ba$ is true. We multiply both left sides of the assumed statement by a^6 in order to obtain an identity 1.

$$\begin{aligned} ab &= ba \\ (a^6)ab &= (a^6)ba \\ (a^6a)b &= a^6ba \\ a^7b &= a^6ba \\ 1b &= a^6ba \\ 1b &= a^6ba \end{aligned}$$

.

Given that a^6 can be expressed as the multiplication of two exponents of a, it holds true that

$$\begin{aligned} 1b &= a^6ba \\ 1b &= a^3a^3ba \\ 1b &= a^3(a^3b)a \end{aligned}$$

.

Employing the given relation twice yields

$$\begin{aligned} 1b &= a^3(a^3b)a \\ b &= a^3(ba^3)a \\ 1b &= (a^3b)a^3a \\ 1b &= (ba^3)a^4 \\ 1b &= ba^7 \\ 1b &= b1 \\ b &= b \end{aligned}$$

. $\square$

Artin Section 4: 4.2

$\Diamond$ An nth root of unity is a complex number z such that $z^n = 1$.

(**a**) Prove that the nth roots of unity form a cyclic subgroup of $\mathbb{C}^\times$ of order n.

(**b**) Determine the product of all the nth roots of unity.

(a)

Proof. To begin, let us define our root of unity z^n to be equal to Euler's identity:

$$z^n = e^{\frac{2\pi i}{n}},\ n = 0, 1, 2, 3, \ldots$$

To demonstrate the cyclic nature of this complex number, we will evaluate $(z^n)^n$ and show that this will indeed map to 1.

$$\begin{aligned}(z^n)^n &= (e^{\frac{2\pi i}{n}})^n \\ &= (e^{\frac{2\pi i n}{n}}) \\ &= (e^{2\pi i}) \\ &= 1.\end{aligned}$$

Thus showing that

$$(z^n)^n = 1.$$

Likewise, the case where the exponent is $l = 0, 1, 2, ..., n-1$ shall be considered to prove that $(z^n)^l$ is infact also a root of unity with order n.

Consider $(z^n)^l$ raised the the power n. The exponenential can be simplified through the laws of exponential algebraic manipulation and substitution to obtain

$$\begin{aligned}((z^n)^l)^n &= ((z^n)^n)^l \\ &= ((e^{\frac{2\pi i}{n}})^n)^l \\ &= (e^{2\pi i})^l \\ &= (1)^l \\ &= 1.\end{aligned}$$

Thus proving that $(z^n)^l$ must be a root of unity for any $l = 0, 1, 2, ..., n-1$.

Therefore, it is indeed true that the nth roots of unity do form a cyclic subgroup of $\mathbb{C}^\times$ of order n, where the group can be described by the generator

$$z^n = \langle e^{\frac{2k\pi i}{n}} \mid n = 0, 1, 2, 3, \ldots \rangle$$

$\square$

(b)

Proof. Drawing upon our solutoin from part a, it was demonstrated that a nth root of unity can be written as a group generated as follows:

$$z^n = \langle e^{\frac{2k\pi i}{n}} \mid n = 0, 1, 2, 3, \ldots \rangle$$

Let us consider writing all the products of the nth roots of unity as follows:

$$\prod_{r=0}^{n-1} z^r = (z^0)(z^1)(z^2) \cdots (z_{n-1}) \tag{1}$$

It should be noted that equation (1) is describing the products of all the roots of the polynomial

$$z^n = 1.$$

Which is equivalent to the binomial

$$z^n - 1 = 0.$$

Thus, the nth root of unity is equivalent to an nth degree polynomial that has $n-1$ distinct roots—given that any root $r \geq n$ can be rewritten as an already existing root.

Because of this astute recharacterization of the nth root of unity, Vieta's formula can be exploited to determine the product of all $n-1$ roots simultaneously.

Recall that Vieta's formula states that for a polynomial of the form

$$x^n - 1 = 0,$$

the product of all roots x_r (excluding the trivial root $x_0 = 0$) can be expressed as the product

$$\prod_{r=1}^{n-1} x^r = (-1)^{n-1}.$$

Due to the root z_0 being equal to 1 for our given polynomial, we may remove it from the considered index and only consider the product from $r = 1$ to $r = n-1$. The resulting product is thus all the products of the roots of unity described by the following alternator:

$$\prod_{r=1}^{n-1} z^r = (-1)^{n-1}.$$

$\square$

Artin Additional Problem 1:

$\Diamond$ Prove that a nonempty subset H of a group G is a subgroup if for all $x, y \in H$, the element xy^-1 is also in H.

Proof. We shall prove that subset H is indeed a subgroup of G—that is we will exemplify how the provided elements of H can be used to prove that the identity element 1, inverses, and needed closure are true in H under the induced multiplicative law of composition of group G.

It is assumed that elements x, y, xy^{-1} are elements that live in subset H, thus $H \neq \emptyset$.

Consider drawing upon an element a that lies in our group G. Let $a = x \in H$ and $a = y \in H$. It can be shown that

$$\begin{aligned} xy^-1 &\in H \\ (a)(a)^{-1} &\in H \\ aa^{-1} &\in H \\ 1 &\in H \end{aligned}$$

Thus, the identity element 1 lives in subset H.

Now, let us consider having $x = 1 \in H$. Then the following holds

$$\begin{aligned} xy^{-1} &\in H \\ 1y^{-1} &\in H \\ y^{-1} &\in H \end{aligned}$$

And given it is assumed that $y \in H$, $y, y^{-1} \in H$.

In a similar fashion, let $x = x^{-1}$ and $y = 1$, then

$$\begin{aligned} xy^{-1} &\in H \\ x^{-1}(1)^{-1} &\in H \\ x^{-1} &\in H \\ x^{-1}1 &\in H \end{aligned}$$

Thus proving that for any element $x, y \in H$, there exist their inverses as well.

Finally, we know that $y^{-1} \in H$, so it is true that

$$\begin{aligned} x(y^{-1})^{-1} &\in H \\ xy &\in H \end{aligned}$$

Thus, H is closed and the subset H is indeed a subgroup of group G. $\square$