

1. INTRODUCTION

This section is about complex numbers. In particular those with absolute value 1.

1.1. complex numbers. Complex numbers are defined to be expressions of the form

$$z = a + bi$$

where $a, b \in \mathbb{R}$ and i is one of the square roots of -1 . Complex numbers are usually denoted by the letter z . Addition and multiplication are defined by

$$(a + bi) + (x + yi) = (a + x) + (b + y)i$$

$$(a + bi)(x + yi) = (ax - by) + (ay + bx)i$$

These operations are associative, commutative and have units.

There is another way to write complex numbers:

$$z = x + yi = re^{i\theta}$$

where these letters are related by

$$x = r \cos \theta, \quad y = r \sin \theta$$

and

$$r = |z| = \sqrt{x^2 + y^2}$$

It is not quite true that $\theta = \tan^{-1} y/x$ since this formula never gives you the angles in the second and third quadrant.

1.2. unit circle. The **unit circle** is given by

$$U = \{x \in \mathbb{C} \mid |z| = 1\}$$

2. BINARY OPERATIONS

A **binary operation** on a set S is defined to be a mapping

$$S \times S \rightarrow S$$

The notation is $(a, b) \mapsto a * b$. In words: for every ordered pair of not necessarily distinct elements (a, b) in the set S the binary operation assigns a unique element $a * b \in S$.

The pair $(S, *)$ is called a **binary structure**.

3. ISOMORPHIC BINARY STRUCTURES

Two binary structures $(S, *)$ and $(T, *)$ are called **isomorphic** if there is a bijection $\phi : S \rightarrow T$ so that

$$\phi(a * b) = \phi(a) * \phi(b)$$

for all $a, b \in S$. This is called the *homomorphism property*. People also say “ ϕ takes multiplication to multiplication.” The notation is $(S, *) \cong (T, *)$.

Example: $(\mathbb{R}, +) \cong (\mathbb{R}_+, \cdot)$. The isomorphism $\phi : \mathbb{R} \rightarrow \mathbb{R}_+$ is given by $\phi(x) = e^x$. The homomorphism property is verified by the properties of exponents:

$$\phi(x + y) = e^{x+y} = e^x e^y = \phi(x)\phi(y)$$

People say: “ ϕ takes addition to multiplication.”

4. GROUPS

A **semigroup** is a set with an associative binary operation.

A **monoid** is a semigroup with a unit e . For example, $(\mathbb{Z}_+, +)$ is a semigroup but not a monoid since the unit 0 is not in the set. On the other hand, the same set is a monoid under multiplication since the multiplicative unit 1 is in the set \mathbb{Z}_+ .

Theorem 4.1. *A binary structure can have at most one two-sided unit. In other words, the unit is unique if it exists.*

Proof. Suppose that u, u' are both units. Then

$$u * u' = u$$

since u' is a right unit and

$$u * u' = u'$$

since u is a left unit. Therefore, $u = u'$. So, any two units are equal. \square

A **group** is a monoid with inverses. By **inverse** we mean a *two-sided inverse*. I.e., b is an inverse for a if

$$a * b = b * a = e \quad (\text{the unit}).$$

An important example of a group is $GL(n, \mathbb{Z})$ under matrix multiplication. This is the group of $n \times n$ invertible matrices with integer entries. From linear algebra we know that integer matrices have integer inverses if and only if its determinant is ± 1 . So $GL(n, \mathbb{Z})$ is also the set of $n \times n$ integer matrices with determinant ± 1 . It is also called the **general linear group**.

4.1. definition of group. We discussed in class one day the more economical definition of a group which requires only a left unit and left inverses.

Theorem 4.2. *Suppose that $(G, *)$ is a binary structure which is associative and has a left unit e and a left inverse g' for every $g \in G$. Then e is also a right unit and g' is also the right inverse for g . Therefore, G is a group.*

Proof. First, note that we have left cancellation: If $xa = xb$ then multiplying on the left with x' gives:

$$a = ea = x'xa = x'xb = eb = b.$$

Next, we show that g' is the right inverse of g . In other words, $gg' = e$. This is the same as saying that g is the left inverse of g' . Let g'' be the left inverse of g' and let g''' be the left inverse of g'' . Then

$$g'''g''g'g = g'''(g''g')g = g'''eg = g'''g$$

$$g'''g''g'g = (g'''g'')(g'g) = ee = e = g'''g''$$

By left cancellation we get $g'' = g$ which shows that g' is a right inverse for g .

Finally, we need to show that e is a right unit:

$$ge = g(g'g) = (gg')g = eg = g.$$

Therefore, G is a group. □

5. SUBGROUPS

A **subgroup** is a subset H of a group G which is closed under the operation (the one that makes G into a group) and which satisfies the definition of a group. Note that associativity is automatic. So, the only assumptions are that $e \in H$ and H is closed under inverse, i.e., if $h \in H$ then $h^{-1} \in H$.

Examples of subgroups are:

- (1) $n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$.
- (2) U_n is a subgroup of (U, \cdot) .
- (3) $SL(n, \mathbb{Z}) < GL(n, \mathbb{Z})$ where $SL(n, \mathbb{Z})$ is the group of $n \times n$ integer matrices with determinant 1.

Theorem 5.1. *A subset H of a group G is a subgroup if and only if it is nonempty and satisfies*

$$H^{-1}H \subseteq H.$$

In class I pointed out that when the same set appears twice in this notation we are supposed to take different elements. Thus

$$H^{-1}H = \{h_1^{-1}h_2 \mid h_1, h_2 \in H\}.$$

Proof. We want to show that H is closed under multiplication, has the unit e and is also closed under inverse. Associativity is automatic since $H \subseteq G$.

- (1) ($e \in H$) Since H is nonempty, it has some element h . Then $h^{-1}h = e \in H^{-1}H \subseteq H$.
- (2) (H is closed under inverse.) Since $e \in H$, $H^{-1} = H^{-1}e \subseteq H^{-1}H \subseteq H$. Also, $H \subseteq H^{-1}$ since each $h \in H$ is equal to $(h^{-1})^{-1} \in H^{-1}$. Thus $H = H^{-1}$.
- (3) (H is closed.) $HH = H^{-1}H \subseteq H$.

Thus, H is a subgroup of G . □

6. CYCLIC GROUPS

Definition 6.1. Suppose that G is a group and $g \in G$. Then the **cyclic subgroup** of G generated by g is defined to be the set of all integer powers of g . It is denoted $\langle g \rangle$. Thus

$$\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$$

The example that I gave was $G = GL(2, \mathbb{Z})$ and

$$\begin{aligned} g &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = g^5 = g^9 = \dots \\ g^2 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = g^6 = g^{10} = \dots \\ g^3 &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = g^7 = g^{11} = \dots \\ g^4 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 = g^8 = g^{12} = \dots \end{aligned}$$

This means that g has order 4.

Definition 6.2. The **order** of an element g of any group is defined to be the smallest positive integer $o(g) = n$ so that $g^n = e$. If there is no such integer n then g has infinite order: $o(g) = \infty$.

In additive notation this is: $ng = 0$.

One of the main results which I remember proving in class is the following important equation.

Theorem 6.3. *If $g \in G$ has order n then*

$$\langle g \rangle \cong \mathbb{Z}_n$$

The way I explained this was with this lemma:

Lemma 6.4. *Suppose that $n = o(g)$. Then the subgroup $\langle g \rangle \leq G$ is equal to the set*

$$\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$$

and there is no repetition in this list of elements.

Proof. By definition, $\langle g \rangle$ consists of all powers g^k of g . But the division algorithm gives

$$k = nq + r$$

where q, r are integers and $0 \leq r \leq n - 1$. So,

$$g^k = g^{qn+r} = g^{qn} g^r = (g^n)^q g^r = e^q g^r = g^r.$$

So, $e, g, g^2, \dots, g^{n-1}$ are all the elements of $\langle g \rangle$.

To see that there are no repetitions suppose that $0 \leq i < j \leq n - 1$ and $g^i = g^j$. Then

$$g^j = g^{j-i+i} = g^{j-i} g^i$$

By right cancellation we get $e = g^{j-i}$. But $1 < j - i < n$. This is a contradiction since n is supposed to be the smallest positive power of g which gives e . Therefore, there are no repetitions in the list. \square

The proof of the theorem follows from this.

Proof of Theorem. Let $\phi : \mathbb{Z}_n \rightarrow \langle g \rangle$ be given by $\phi(k) = g^k$. The lemma says that this is a bijection. So we only need to verify the homomorphism property (HP).

Let $i, j \in \mathbb{Z}_n$. Then, there are two cases. Either $i + j < n$ or $i + j \geq n$.

Case 1. If $i + j < n$ then $\phi(i)\phi(j) = g^i g^j = g^{i+j} = \phi(i + j)$

Case 2. If $i + j \geq n$ then $i +_n j = i + j - n$. Then

$$\phi(i +_n j) = \phi(i + j - n) = g^{i+j-n} = g^i g^j g^{-n} = g^i g^j = \phi(i)\phi(j).$$

So, in both cases, the HP holds. Thus ϕ is an isomorphism as claimed. \square