Artin's Algebra

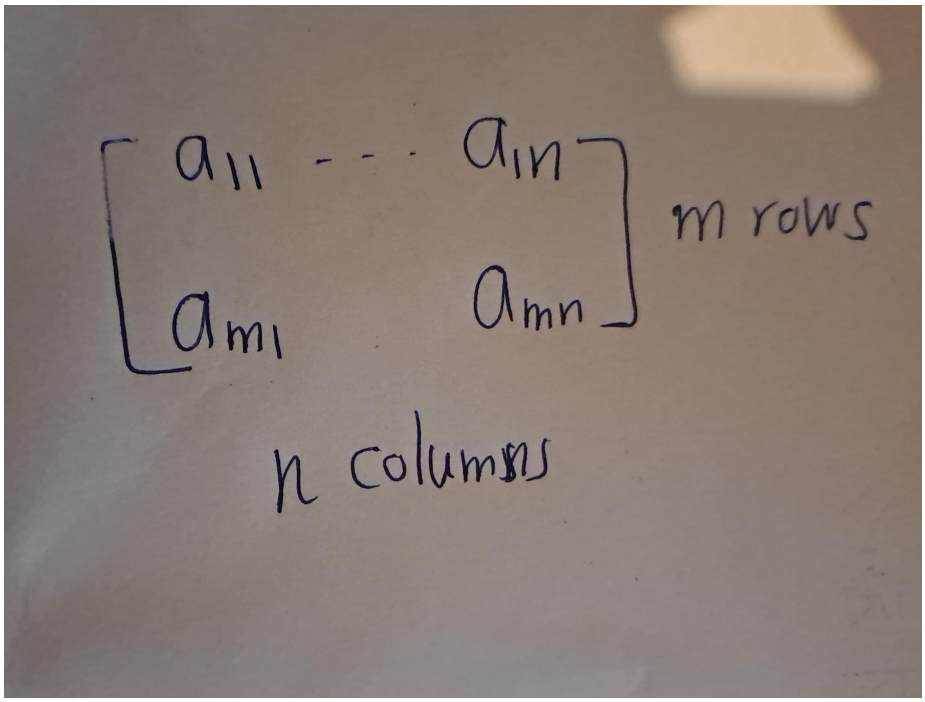
Ashan Jayamal

2024-04-02

Matrices

Basic Operations

Let m and n be positive integers. An $m \times n$ matrix is a collection of mn numbers arranged in a rectangular array.



::: {.example #unnamed-chunk-1}

$$A := \begin{bmatrix} 8 & 0 & 3 \\ 78 & -5 & 2 \end{bmatrix}$$

A is 2×3 matrix.(two rows and three columns)

::: The numbers in a matrix are the matrix entries. They may be denoted by a_{ij}, where i and j are indices (integers) with $1 < i < m$ and $1 < j < n$. The index i represents the row index, and j represents the column index. So a_{ij} is the entry that appears in the ith row and jth column of the matrix.

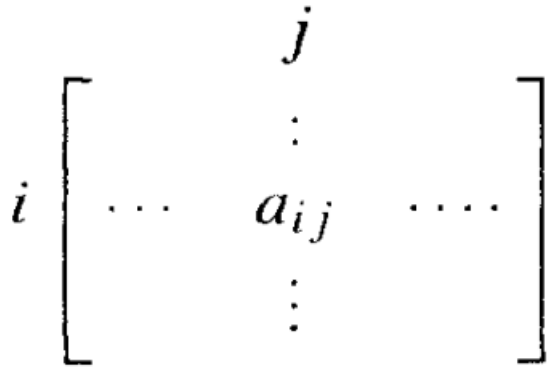


Figure 1:

Group Theory

Laws of Compositions

A law o f composition on a set S is any rule for combining pairs a, b of elements of S to get another element, say p, of S.

- Some models for this concept are addition and multiplication of real numbers.
- Matrix multiplication on the set of $n \times n$ matrices is another example.

Formally, a law of composition is a function of two variables, or a map,

$$S \times S \to S$$

Here, $S \times S$ denotes, as always, the product set, whose elements are pairs a, b of elements of S.

The element obtained by applying the law to a pair a, b is usually written using a notation resembling one used for multiplication or addition:

$$p = ab, a \times b, a \circ b, a + b$$

, or whatever, a choice being made for the particular law in question. The element p may be called the product or the sum of a and b, depending on the notation chosen.

Groups and Subgroups

A group is a set G together with a law of composition that has the following properties:

- The law of composition is associative: $(ab)c = a(bc)$ for all a, b, c in G.

- G contains an identity element 1, such that $la = a$ and $al = a$ for all a in G.
- Every element a of G has an inverse, an element b such that $ab = 1$ and $ba = 1$.

Notation: If set G with composition $\cdot$ is a group, then we denote it by $(G, \cdot)$ ::: {.definition #unnamed-chunk-5 name="Ableian Group"} Group G is called abliean if its law of composition is commutative. i.e.

$$\forall x \in G, xy = yx$$

:::

- $\mathbb{R}^\times := \mathbb{R} \setminus \{0\}$ is an abliean group under multiplication
- $GL_n(\mathbb{R}) := \{A \in M_n(\mathbb{R}) : \text{ A is invertible}\}$ with materix multiplication is non-abliean group. This group is called *general linear group*.

The order of a group G is the number of elements that it contains. We

$$|G| := \text{number of elements of } G = \text{ the order of G}$$

If the order is finite, G is said to be a finite group. If not, G is an infinite group.

Here is our notation for some familiar infinite abelian groups:

- $(\mathbb{Z}, +)$:The set of integers, with addition as itslaw of composition (the additive group of integers)
- $(\mathbb{R}, +)$:The set of real numbers, with addition as its law of composition (the additive group of real numbers)
- $(\mathbb{R}^\times, \times)$:The set of nonzero real numbers, with multiplication as its law of composition(the multiplicative group) $(\mathbb{C}, +)$:the set of complex numbers, with addition as its law of composition (the additive group of complex numbers)
- $(\mathbb{C}^\times, \times)$:The set of nonzero complex numbers, with multiplication as its law of composition(the multiplicative group of complex numbers)

Let G be group and let $a, b, c \in G$ whose law of composition is written multiplicatively.

- If $ab = ac$ or if $ba = ca$, then $b = c$.
- If $ab = a$ or if $ba = a$, then $b = 1$

Multiply both sides of $ab = ac$ on the left bya^{-1} to obtain $b = c$. The other proofs are analogous.

As you saw a^{-1} plays amajor rule in above proof. So the cancelation rule does not holds when elemenet a is not invertible.

$$\begin{bmatrix}1 & 1\\0 & 0\end{bmatrix}\begin{bmatrix}1 & 1\\2 & 0\end{bmatrix}=\begin{bmatrix}1 & 1\\0 & 0\end{bmatrix}\begin{bmatrix}3 & 0\\0 & 1\end{bmatrix}$$

Let T be a set and $G := \{f : T \to T : f \text{ is a bijection}\}$. Then G with composition is a group. We use notation \$sys(T) \$ to denote the

The group of permutations of the set of indices $\{l, 2, ..., n\}$ is called the *symmetric group*,and is denoted by S_n. Then $|S_n| = n!$. So, S_n is a finite group of order $n!$.

Let's disscuss some individualcases for n.

- $n = 2$
  The permutations of a set $\{1, 2\}$ of two elements are the identity i and the transposition $\tau = (12)$.
  $$S_2 := \{id, (12)\}$$

$\circ$	id	(12)
id	id	(12)
(12)	(12)	id

- $n = 3$
  S_3 has order $3! = 6$. S_3 serves as a convenient example because it is the smallest group whose law of composition isn't commutative. We will refer to it often. To describe it, we pick two particular permutations in terms of which we can write all others. We take the cyclic permutation (123), and the transposition (12), and label them as x and y, respectively.Then

  $$x^3 = (123)^3 = (123)(123)(123) = (123)(132) = id \quad (1)$$
  $$y^2 = (12)^2 = (12)(12) = id \quad (2)$$
  $$yx = (12)(123) = (13) = (132)(12) = ((123)(123))(12) = (123)^2(12) \quad (3)$$

  As a summary,
  $$x^3 = 1, Y^2 = 1, yx = x^2y$$

Subgroups of the Additive Group of Integers

We review some elementary number theory here, in terms of subgroups of the additive group $\mathbb{Z}^+$ of integers. To begin, we list the axioms for a subgroup when additive notation is used in the group: A subset S of a group G with law of composition written additively is a subgroup if it has these properties:

- *Closure* : If a and b are in S, then $a + b$ is in S.
- *Identity* : 0 is in S.
- *Inverses* : If a is in S then $-a$ is in S.

Let a be an integer different from O. We denote the subset of $\mathbb{Z}$ that consists of all multiples of a by $a\mathbb{Z}$:

$$a\mathbb{Z} := \{n \in \mathbb{Z} | n = ka \text{ for some } k \in \mathbb{Z}\}$$

.

This is a subgroup of $\mathbb{Z}^+$. Its elements can also be described as the integers divisible by a.

Let S be a subgroup of the additive group $\mathbb{Z}^+$. Either S is the trivial subgroup $\{0\}$, or else it has the form $a\mathbb{Z}$, where a is the smallest positive integer in S.

Let S be a subgroup of $\mathbb{Z}^+$. Then $0 \in S$, and if 0 is the only element of S then S is the trivial subgroup. ie.: $S = \{0\}$So that case is settled.

Otherwise, S contains an integer n different from 0, and either n or $-n$ is positive. The third property of a subgroup tells us that $-n$ is in S, so in either case, S contains a positive integer. We must show that S is equal to $a\mathbb{Z}$, when a is the smallest positive integer in S.

We first show that $a\mathbb{Z}$ is a subset of S, in other words, that ka is in S for every integer k. If k is a positive integer, then $ka = a + a + \cdots + a$ (k terms). Since a is in S, closure and induction show that ka is in S. Since inverses are in S, $-ka$ is in S. Finally, $0 = 0a$ is in S.

Next we show that S is a subset of Za, that is, every element n of S is an integer multiple of a. We use division with remainder to write $n = qa + r$, where q and r are integers and where the remainder r is in the range $0 < r < a$. Since Za is contained in S, qa is in S, and of course n is in S. Since S is a subgroup, $r = n - qa$ is in S too. Now by our choice, a is the smallest positive integer in S, while the remainder r is in the range $0 < r < a$. The only remainder that can be in S is 0. So $r = 0$ and n is the integer multiple qa of a.

Cyclic Groups

Homomorphisms

Let $(G, *)$ and $(G', \odot)$ be groups. A **homomorphism** $\phi : G \to G'$ is a map from G to G' such that for all a and b in G:

$$\phi(a * b) = \phi(a) \odot \phi(b). \tag{4}$$

Examples of Homomorphisms

1. **Determinant Function**: $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$
2. **Exponential Map**: $\exp : (\mathbb{R}, +) \to (\mathbb{R}^\times, \times)$ defined by $x \mapsto e^x$
3. **Map** ϕ: $(\mathbb{Z}, +) \to G$ defined by $\phi(n) = a^n$, where a is a given element of G
4. **Absolute Value Map**: $|\cdot| : (\mathbb{C}^\times, \times) \to (\mathbb{R}^\times, \times)$

Trivial Homomorphism

The trivial homomorphism $\phi : G \to G'$ between any two groups maps every element of G to the identity in G'.

Inclusion Map

If H is a subgroup of G, the inclusion map $i : H \to G$ defined by $i(x) = x$ for x in H is a homomorphism.

Let $\phi : G \to G'$ be a group homomorphism.

(a) If $a_i, \ldots, a_k$ are elements of G, then $\phi(a_i \ldots a_k) = \phi(a_i) \ldots \phi(a_k)$.

(b) ϕ maps the identity to the identity: $\phi(1_G) = 1_{G'}$.

(c) ϕ maps inverses to inverses: $\phi(a^{-1}) = \phi(a)^{-1}$.

Let $\phi : G \to G'$ be a homomorphism of groups, and let $a, b \in G$. Let $K \ker(\phi)$. Then following conditions are equivalent:

- $\phi(a) = \phi(b)$,
- $a^{-1}b$ is in K,
- b is in the coset aK,
- The cosets bK and aK are equal.

- (1) $\implies$ (2).\ Suppose $\phi(a) = \phi(b)$. Now consider

$$\phi(a^{-1}b) = \phi(a^{-1})\phi(b) = \phi(a^{-1})\phi(b) = 1$$

  Thus, $a^{-1}b \in K$.
- (2) $\implies$ (1)\ If $a^{-1}b \in K$

$$1 = \phi(a^{-1}b) = \phi(a^{-1})\phi(b) = \phi(a^{-1})\phi(b)$$

  . Thus, $\phi(a) = \phi(b)$. (3) $\implies$ (4)
- Suppose b is in the coset aK. Then $b = ak$ for some

Isomorphisms

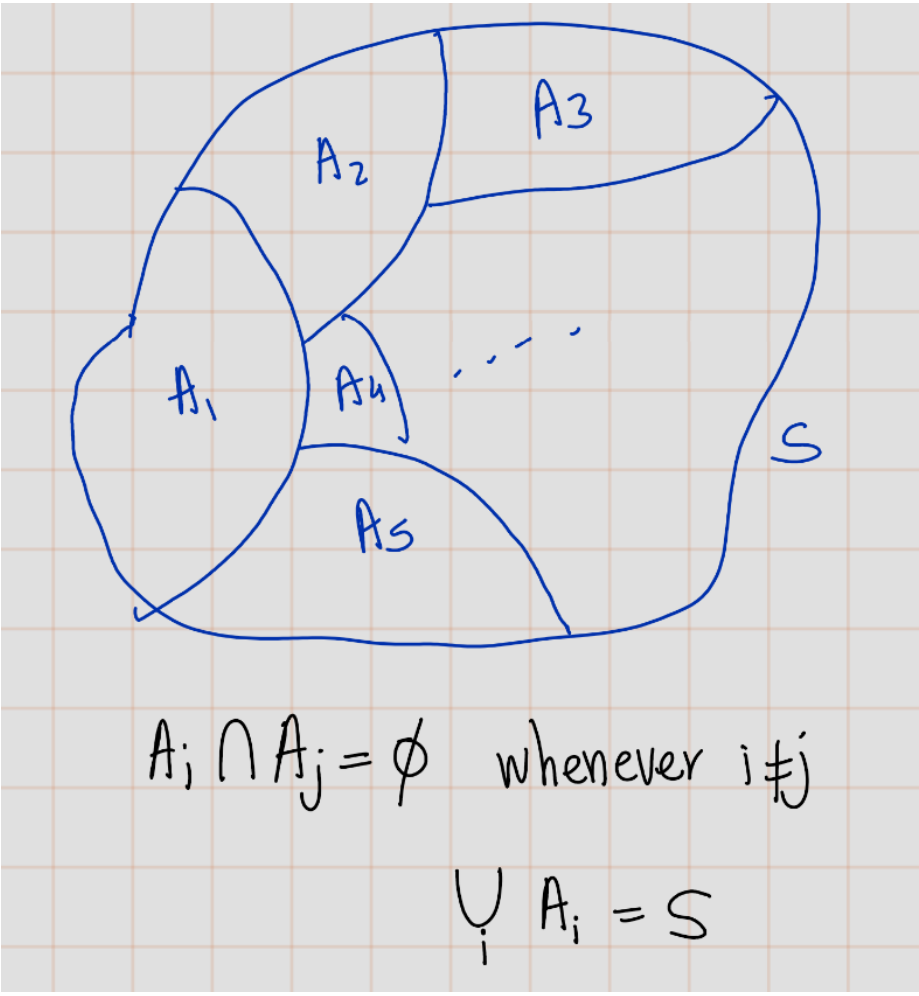
Equivalence Relations and Partitions

Sure, here is the LaTeX version of your statement:

A partition n of a set S is a subdivision of S into nonoverlapping, nonempty subsets:

$$S = \bigcup_i A_i$$

,where A_i are disjoint nonempty subsets of S.



The two sets *Even* and *Odd* partition the set of integers.

With the usual notation, the sets

$$\{1\}, \{y, xy, x^2y\}, \{x, x^2\}$$

form a partition of the symmetric group S_3.

An equivalence relation on a set S is a relation that holds between certain pairs of elements.

- Reflexive: For all a, $a \sim a$.
- Symmetric: If $a \sim b$, then $b \sim a$.
- Transitive: If $a \sim b$ and $b \sim c$, then $a \sim c$.

Two triangles are said to be congruent if their sides have the same length and angles have same measure.
Congruence of triangles is an example of an equivalence relation on the set of triangles in the plane. If A, B, and C are triangles, and if A is congruent to B and B is congruent to C, then A is congruent to C. It is very easy to check three equivalnace propoties. I am not going to do this.

Conjugacy is an equivalence relation on a group. Let G be garoup Two group elements are conjugate, $a \sim b$, if $b = gag^{-1}$ for some $g \in G$.

- *Reflexive*: Observe that $a = aaa^{-1}$ then, $a \sim a$.
- *Symmetric*: Suppose that $a \sim b$, then $b = gag^{-1}$. Thus, $a = g^{-1}bg$. Hence, $b \sim a$.
- *Transitive*: Suppose that $a \sim b$ and $b \sim c$. This means that $b = g_1 a g_1^{-1}$ and $c = g_2 b g_2^{-1}$ for some group elements g_1 and g_2. Then $c = g_2(g_1 a g_1^{-1})g_2^{-1} = (g_2 g_1)a(g_2 g_1)$, so $a \sim c$

An equivalence relation on a set S determines a partition of S, and conversely.

- ($\Longrightarrow$): Given a partition of S, the corresponding equivalence relation is defined by the rule that $a \sim b$ if a and b lie in the same subset of the partition. The axioms for an equivalence relation are obviously satisfied.
- ($\Longrightarrow$): Given an equivalence relation ($\sim$), one defines a partition this way: The subset that contains a is the set of all elements b such that $a \sim b$. This subset is called the **equivalence class** of a. We'll denote it by C_a here

  $$C_a = \{b \in S | a \sim b\}$$

  The next lemma completes the proof of the proposition

Given an equivalence relation on a set S, the subsets of S that are equivalence classes partition S.

This is an important point, so we will check it carefully. We must remember that the notation C_a stands for a subset defined in a certain way. The partition consists of the subsets, and several notations may describe the same subset.

- *Non-emptyness*: The reflexive axiom tells us that a is in its equivalence class. Therefore, the class C_a is nonempty.
- *Union is whole set*: Since a can be any element, the union of the equivalence classes is the whole set S.
- *Disjoint property*: To show this, we prove follwoing calim:
  - **Claim**: If C_a and C_b have an element in common, then $C_a = C_b$. Since we can interchange the roles of a and b, it will suffice to show that if C_a and C_b have an element, say d, in common, then $C_b \subseteq C_a$. Sippose that x is in C_b, then $b \sim x$. Since d is in both sets, $a \sim d$ and $b \sim d$, and the symmetry property tells us that $d \sim b$. So we have $a \sim d$, $d \sim b$, and $b \sim x$. Two applications of transitivity show that $a \sim x$, and therefore, x is in C_a.

The relation on a group defined by $a\ b$ if a and b are elements of the same order is an equivalence relation. (Trivial.)

The corresponding partition for the symmetric group S3 are

$$\{1\}, \{y, xy, x^2y\}, \{x, x^2\}.$$

If a partition of a set S is given, we may construct a new set $\overline{S}$ whose elements are the subsets. We imagine putting the subsets into separate piles, and we regard the piles as the elements of our new set $\overline{S}$. It seems advisable to have a notation to distinguish a subset from the element of the set S (the pile) that it represents. If U is a subset, we will denote by $[U]$ the corresponding element of S.

If S is the set of integers and if Even and Odd denote the subsets of even and odd integers, respectively, then $\overline{S}$ contains the two elements [Even] and [Odd].

We will use this notation more generally. When we want to regard a subset U of S as an element of a set of subsets of S, we denote it by $[U]$.

When an equivalence relation on S is given, the equivalence classes form a partition, and we obtain a new set $\overline{S}$ whose elements are the equivalence classes $[C_a]$. We can think of the elements of this new set in another way, as the set obtained by changing what we mean by equality among elements. If a and b are in S, we interpret $a \sim b$ to mean that a and b become equal in $\overline{S}$, because $C_a = C_b$. With this way of looking at it, the difference between the two sets S and $\overline{S}$ is that in $\overline{S}$ more elements have been declared "equal," i.e., equivalent. It seems to me that we often treat congruent triangles this way in school.

For any equivalence relation, there is a natural surjective map

$$\pi : S \to \overline{S} \tag{5}$$

that maps an element a of S to its equivalence class: $\pi(a) = [C_a]$. When we want to regard $\overline{S}$ as the set obtained from S by changing the notion of equality, it will be convenient to denote the element $[C_a]$ of $\overline{S}$ by the symbol a. Then the map π becomes

$$\pi(a) = \overline{a} \tag{6}$$

We can work in $\overline{S}$ with the symbols used for elements of S, but with bars over them to remind us of the new rule:

$$\text{If } a \text{ and } b \text{ are in } S, \text{ then } \overline{a} = \overline{b} \text{ means } a \sim b. \tag{7}$$

A disadvantage of this bar notation is that many symbols represent the same element of S. Sometimes this disadvantage can be overcome by choosing a particular element, a representative element, in each equivalence class. For example, the even and the odd integers are often represented by $\overline{0}$ and $\overline{1}$:

$$\{[\text{Even}], [\text{Odd}]\} = \{\overline{0}, \overline{1}\}. \tag{8}$$

Though the pile picture may be easier to grasp at first, the second way of viewing S is often better because the bar notation is easier to manipulate algebraically.

The Equivalence Relation Defined by a Map

Any map of sets $f : S \to T$ gives us an equivalence relation on its domain S. It is defined by the rule: $a \sim b$ if $f(a) = f(b)$.

The inverse image of an element t of T is the subset of S consisting of all elements s such that $f(s) = t$. It is denoted symbolically as

$$f^{-1}(t) = \{s \in S \mid f(s) = t\}. \tag{9}$$

The inverse images are also called the fibres of the map f , and the fibres that are not empty are the equivalence classes for the relation defined above.

This is symbolic notation. Please remember that **unless f is bijective, f^{-1} will not be a map**.

Here the set S of equivalence classes has another incarnation, as the image of the map. The elements of the image correspond bijectively to the nonempty fibres, which are the equivalence classes

Let's consider the absolute value map from the complex numbers $\mathbb{C}^\times$ to the positive real numbers $\mathbb{R}^+$:

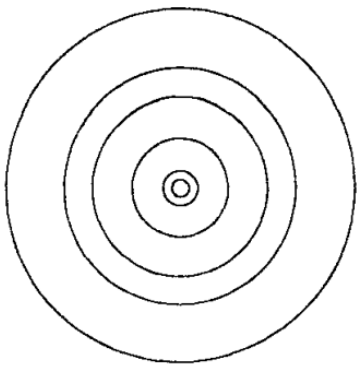
$$f : \mathbb{C}^\times \to \mathbb{R}^+, \quad f(z) = |z|$$

The fiber of an element t in $\mathbb{R}^+$ is the subset of $\mathbb{C}^\times$ consisting of all complex numbers z such that $f(z) = |z| = t$. Symbolically, we denote the fiber as:

$$f^{-1}(t) = \{z \in \mathbb{C}^\times : |z| = t\}$$

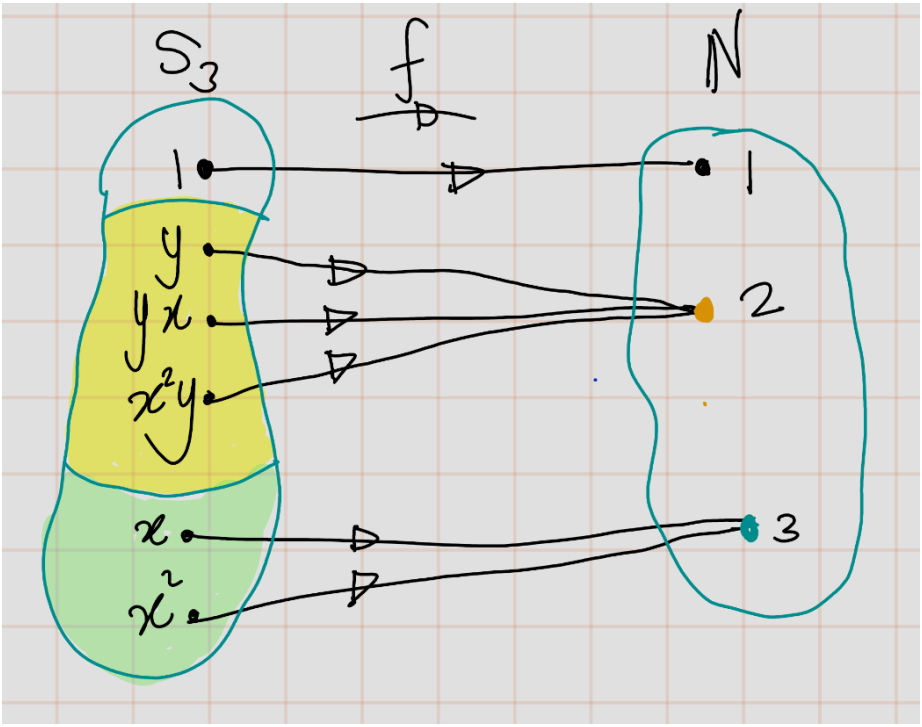
This fiber represents all complex numbers with the same absolute value t. Thus, fibers are circles in Complex plane.

Note that the absolute value map is surjective, so each positive real number t corresponds to a unique fiber in $\mathbb{C}^\times$.



Some Fibres of the Absolute Value Map $\mathbb{C}^\times \to \mathbb{R}^\times$.

If G is a finite group, we can define a map $f : G \to \mathbb{N}$ to the set $\{1, 2, 3, \ldots\}$ of natural numbers, letting $f(a)$ be the order of the element a in G. The fibers of this map are the sets of elements with the same order (see example @ref(exm:272)).

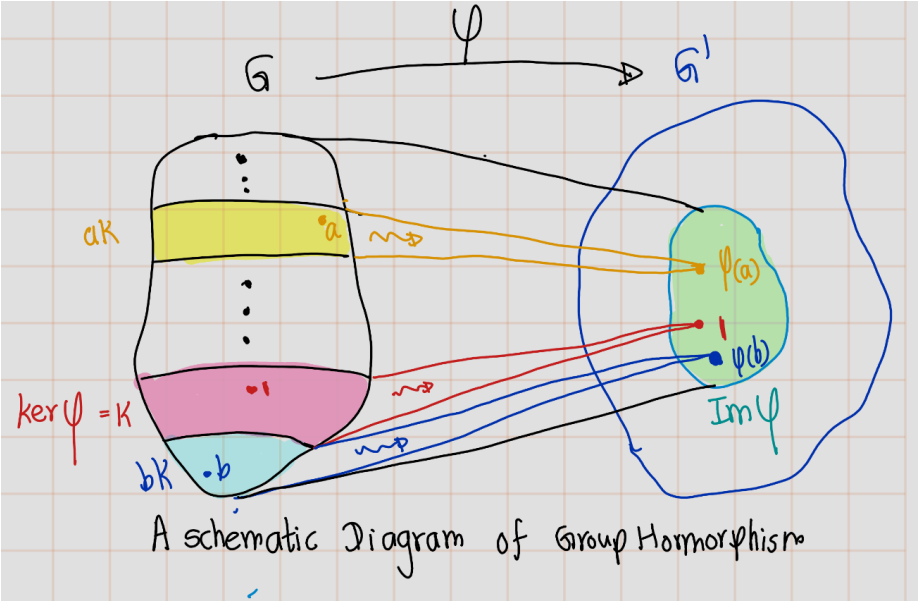


Let G, G' be a groups and $\phi : G \to G'$ be a group group homomorphism. The equivalence relation on G defined by ϕ is usually denoted by $\equiv$, rather than by $\sim$, and is referred to as congruence.

$$a \equiv b \text{ if } \phi(a) = \phi(b)$$

We have seen that elements a and b of G are congruent, i.e., $\phi(a) = \phi(b)$, if and only if b is in the coset aK of the kernel K (See proposition @ref(prp:258))

Let K be the kernel of a homomorphism $\varphi : G \to G'$. The fibre of that contains an element a of G is the coset aK of K. These cosets partition the group G, and they correspond to elements of the image of φ.



The fibre of φ over an element $g' \in G'$ is the set of all elements $a \in G$ such that $\varphi(a) = g'$. Let's denote this fibre as

$$F_{g'} = \{a \in G : \varphi(a) = g'\}$$

.

Now, let's take an arbitrary element $a \in G$ and consider the left coset $aK = \{ak : k \in K\}$.

We know that K is the kernel of φ, so for any $k \in K$, we have $\varphi(k) = 1_{G'}$ where $1_{G'}$ is the identity element in G'.

- Claim 1: $aK = F_{\varphi(a)}$.
  - sub claim 1.1: $aK \subseteq F_{\varphi(a)}$.
    For any $ak \in aK$, we have $\varphi(ak) = \varphi(a)\varphi(k) = \varphi(a)1_{G'} = \varphi(a)$.This shows that every element in the coset aK is mapped to the same element under φ as a itself. Therefore, the coset aK is a subset of the fibre $F_{\varphi(a)}$.
  - sub claim 1.2 : $F_{\varphi(a)} \subseteq aK$.
    If $a' \in F_{\varphi(a)}$, then $\varphi(a') = \varphi(a)$, which implies that $\varphi((a')^{-1}a) = 1_{G'}$. This means that $(a')^{-1}a \in K$, or equivalently, $a' \in aK$. (by proposition @ref(prp:258))Therefore, the fibre $F_{\varphi(a)}$ is a subset of the coset aK.

Since aK is a subset of $F_{\varphi(a)}$ and $F_{\varphi(a)}$ is a subset of aK, we conclude that $aK = F_{\varphi(a)}$. So, the fibre of φ that contains an element a of G is indeed the coset aK of K.

- Claim 2: The cosets of a subgroup K partition the group G.

A partition of a set is a collection of non-empty subsets such that every element in the set is in exactly one of these subsets.

To show that the cosets of K partition G, we need to show two things:

- sub claim 2.1: Every element of G is in at least one coset of K.
  Given any $g \in G$, g is in the coset gK. So, every element of G is in at least one coset of K.
- sub claim 2.2: No element of G is in more than one coset of K
  Suppose gK and hK are two cosets of K and there is some element $x \in G$ that is in both gK and hK. This means that there exist $k_1, k_2 \in K$ such that $x = gk_1 = hk_2$ (by proposition @ref(prp:258). Then $g = hk_2k_1^{-1}$. Thus, $g \in gK$, which implies that $gK = hK$. So, no element of G is in more than one coset of K.

Therefore, the cosets of K partition the group G.

Cosets

Modular Arithmetic

The Correspondence Theorem

Let $\phi : G \to G'$ be a group homomorphism, and let H be a subgroup of G. We may restrict ϕ to H, obtaining a homomorphism

$$\phi|_H : H \to G'$$

In other words, we take the same map but restrict its domain.

Notation: We use this notation for clarity $[\phi|_H](h)$.

Further, we can see that follwoing observatons.

- By definition, $\forall h \in H, \phi|_H(h) = \phi(h)$
- The restriction $\phi|_H$ is a homomorphism (Since ϕ is homomorphism).
- The kernel of $\phi|_H$ is the intersection of the kernel of ϕ with H:

  $$ker(\phi|_H) = (ker\phi) \cap H$$

  There is no need to prove this. This is trivial by definition of kernel.

- Image of $\phi|_H$ is the same as the image $\phi(H)$ of H under the map ϕ.

$$Im(\phi_H) = \phi(H)$$

- If $|H|$ and $|G'|$ have no common factor, $\phi(H) = \{1\}$, so H is contained in the kernel. (Since, by Artin's book corollary 2.8.13,

$$|Im(\phi_H)| \mid |H| \tag{10}$$

$$|Im(\phi_H)| \mid |G'| \tag{11}$$

, Thus, if $|H|$ and $|G'|$ have no common factors,$|Im(\phi_H)| = |\phi(H)| = 1$. So, $Im(\phi_H) = \phi(H) = \{1\}$

Now let's see an example.

Define sign homorphism $\sigma : S_n \to \{\pm 1\}$ by $\sigma(x) = 1$ if x is even, and $\sigma(x) = -1$ if x is odd. Then the image of the sign homomorphism is,

$$Im(\sigma) = \{\pm 1\}$$

it has order 2.

Let $H = \{x \in S_n : \text{if } x \text{ has odd order}\}$. Then H is a subgroup. So,, $H \subset \ker(\sigma)$ (We can easily verify this.)

Furthur, The sub group of S_n with even permutations is called *Alternating group* (A_n).

PROBLEM

Let $\phi : G \to G'$ be a homomorphism with kernel K, and let $H' \leq G'$. Denote the inverse image $\phi^{-1}(H')$ by H. i.e.:

$$H = \phi^{-1}(H') = \{x \in G : \phi(x) \in H'\}$$

Then,

- $\phi^{-1}(H')$ is a subgroup of G that contains K.
- If H is a normal subgroup of G', then $\phi^{-1}(H')$ is also a normal subgroup of G.
- If ϕ is surjective and H is a normal subgroup of G, then $\phi^{-1}(H')$ is a normal subgroup of G'.

ϕ^{-1} is not a map.

- **Claim 1**: $K \subseteq \phi^{-1}(H') = H$
  Let $x \in K$. Then $\phi(x) = 1_{G'}$. Since $1_{G'} \in H'$. Thus, $x \in \phi^{-1}(H') = H$. Therfore, $K \subseteq \phi^{-1}(H') = H$
- **Claim 2**: $\phi^{-1}(H')$ is a subgroup of G

  - *Closure* :Suppose $x, y \in H = \phi^{-1}(H')$. Then $\phi(x), \phi(y) \in \phi(H')$. Since ϕ is hormophism $\phi(x)\phi(y) = \phi(xy)$. Since $H' \leq G'$, then $\phi(xy) = \phi(x)\phi(y) \in H'$. Thus, $xy \in \phi^{-1}(H') = H$
  - *Identity* : Since $\phi(1_G) = 1_{G'}$, $1_G \in \phi^{-1}(H') = H$
  - *Inverse* : Let $x \in \phi^{-1}(H') = H$. Then $\phi(x) \in H'$ and since $H' \leq G'$,then $(\phi(x))^{-1} \in H'$. Since ϕ is a homomorphism, $(\phi(x))^{-1} = \phi(x^{-1})$, Thus $(\phi(x))^{-1} = \phi(x^{-1}) \in H'$. Hence, $x^{-1} \in \phi^{-1}(H')$.

- **Claim 3**: If H' is a normal subgroup of G', then $\phi^{-1}(H')$ is also a normal subgroup of G.
  Now suppose that H' is a normal subgroup of G'. Let $x \in H$ and $g \in G$. Then, since ϕ is hormorphism,

  $$\phi(-1) = \phi(g)\phi(x)\phi(g^{-1}) = \phi(g)\phi(x)(\phi(g))^{-1}$$

  So, $\phi(gxg^{-1})$ is conjugate of $\phi(x)$. Since $x \in H = \phi^{-1}(H')$,the $\phi(x) \in H'$. Thus, $\phi(gxg^{-1}) = \phi(g)\phi(x)(\phi(g))^{-1} \in H'$. Hence, $gxg^{-1} \in \phi^{-1}(H') = H$.
- **Claim 4**: If ϕ is surjective and H is a normal subgroup of G, then $\phi^{-1}(H')$ is a normal subgroup of G'.
  Suppose that ϕ is surjective and H is a normal subgroup of G. Let $a \in H'$ and $b \in G'$. Since ϕ is surjcetive, There are elements $x \in H$ and $y \in G$ such that $\phi(x) = a$ and $\phi(y) = b$. Since H is normal $yxy^{-1} \in H$, thus $\phi(yxy^{-1}) = bab^{-1} \in H'$.

let denote the determinant homomorphism

$$det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$$

. Note that $\mathbb{R}^+ \trianglelefteq \mathbb{R}^\times$. (It is very clear that \$The set of positive real numbers is a subgroup of $\mathbb{R}^\times$, and since $\mathbb{R}^\times$ is abliean, $\mathbb{R}^+$ is normal.) Now consider the inverse image of $\mathbb{R}^+$,

$$det^{-1}(\mathbb{R}^+) = \{A \in GL_n(\mathbb{R}) : det(A) \in \mathbb{R}^+\} = SL_n(\mathbb{R})$$

. By above proposition we can ge that $SL_n(\mathbb{R})$ is normal subgroup. (Because $\mathbb{R}^+ \trianglelefteq \mathbb{R}^\times$ and *det* is surjective map.)

Let $\phi : G \to G'$ be a surjective group homomorphism with kernel K. There is a bijective correspondence between subgroups of G' and subgroups of G that contain K:

$$\{\text{subgroups of } G \text{ that contain } K\} \longleftrightarrow \{\text{subgroups of } G'\}$$

This corresponde nce is defined as follows:

$$\begin{aligned} \text{a subgroup } H \text{ of } G \text{ that contains K} &\rightsquigarrow \text{ its image}(\phi(H) \in G', \\ \text{a subgroup } H' \text{ of } G' &\rightsquigarrow \text{ its inverse image } \phi^{-1}(H') \text{ in } G. \end{aligned}$$

- If H and H' are corresponding subgroups, then H is normal in G if and only if is normal in G'.
- If If H and H' are corresponding subgroups, then

$$|H| = |H'||K|$$

Let H be subgroup of G that contain K. Let H' be a subgroup of G'. Now we need to check folllwings,

- $\phi(H)$ is a subgroup of G'.
- $\phi^{-1}(H')$ is a subgroup of G, and it contains K.
- H' is a normal subgroup of G' if and only if $\phi^{-1}(H')$ is a normal subgroup of G.
- (*bijectivity of the correspondence*) $\phi(\phi^{-1}(H')) = H'$ and $\phi^{-1}(\phi(H)) = H$
- $|(\phi^{-1}(H')| = |H'||K|$.
- **Claim 1**: $\phi(H)$ is a subgroup of G'.
  - *Closure*: Let $\$x, y \in phi(H)$. Then there is $a, b \in H$ such that $\phi(a) = x$ and $\phi(b) = y$. Since ϕ is hormorphism, $xy = \phi(a)\phi(b) = \phi(ab)$. Sine $H \leq G$, $ab \in H$, $xy = \phi(ab) \in \phi(H)$.
  - *Identity* : Since $1_G \in H$, $\phi(1_G) = 1_{G'} \in \phi(H)$
  - *Inverse* : Let $x \in \phi(H)$. Then there exist $a \in H$ such that $\phi(a) = x$. Since $H \leq G$, a^{-1} exists in H. $\phi(a^{-1}) = \phi(a)^{-1} = x^{-1} \in \phi(G)$.
- **Claim 2**: $\phi^{-1}(H')$ is a subgroup of G, and it contains K.
  This is true from proportion @ref(prp:2104)
- **Claim 3**: H' is a normal subgroup of G' if and only if $\phi^{-1}(H')$ is a normal subgroup of G.
  Alreday this prooved in proportion @ref(prp:2104)
- **Claim 4.1**: $\phi(\phi^{-1}(H')) = H'$
  - $\phi(\phi^{-1}(H')) \subset H'$
    Lett $x \in \phi(\phi^{-1}(H'))$. Then there exist $y \in \phi^{-1}(H')$ such that $\phi(y) = x$. Then by definiton of the pre image $x = \phi(y) \in H'$.

- $\phi(\phi^{-1}(H')) \supset H'$
  Let $a \in H'$. Since ϕ is surjective, there exists $b \in G$ such that $\phi(b) = a \in H'$. Thus $b \in \phi^{-1}(H')$. Hence $a = \phi(b) = \phi(\phi^{-1}(H'))$.

Therefore, $\phi(\phi^{-1}(H')) = H'$.

- **Claim 4.2**: $\phi^{-1}(\phi(H)) = H$
  - $\phi^{-1}(\phi(H)) \supset H$
    Let $x \in H$. Then $\phi(x) \in \phi(H)$. So, $x \in \phi^{-1}(\phi(H))$.
  - $\phi^{-1}(\phi(H))subsetH$
    Let $y \in \phi^{-1}(\phi(H))$. By definition of inverse image, $\phi(y) \in \phi(H)$. Then there exist $z \in H$ such that $\phi(y) = \phi(z)$. Then $z^{-1}y$ is in the kernal K.(by Artins book proposition 2.5.8). Since $K \subset H$, $z^{-1}y \in H$. So, $a \in H$ and $a^{-1}z \in H$. Thus, $a(a^{-1}x) = x \in H$. Hence $\phi^{-1}(\phi(H)) \subset H$

Therefore, $\phi^{-1}(\phi(H)) = H$ - **Claim 5** : $|(\phi^{-1}(H')| = |H'||K|$.

Problem

Recall

$S_4 = \{id, (12), (13), (14), (23), (24), (34), (123), (124), (132), (134), (142), (143), (234), (1234)\}$
$S_3 = \{id, (12), (13), (23), (123), (132)\}$

There are 6 such subgroups of S_3,

$$< (12) >, < (13) >, < (23) >, < (123) >=< (132) >, S_3$$

. There is one proper subgroup of order 3. That is $< (123) >$. There are 3 subgroups of order 2. They are $< (12) >, < (13) >, < (23) >$

The Correspondence Theorem tells us that there are four proper subgroups of S_4 that contain K.

Problem

Product Groups

Let G, G' be two groups. The product set $G \times G'$, the set of pairs of elements (a, a') with a in G and a' in G', can be made into a group by component-wise multiplication,

multiplication of pairs is defined by the rule,

$$(a, a') \cdot (b, b') = (ab, a'b') \quad \text{for } a, b \in G \text{ and for } a', b' \in G$$

Let's prove that $G \times G'$ is a group.

Let G, G' be two groups and let $a, b, c \in G$ and $a', b', c' \in G'$

- *Closure* : $(a, a') \cdot (b, b') = (ab, a'b')$. So, since $a, b \in G$ and $a', b' \in G'$ and G and G' be a group, then $ab \in G$ and $a'b' \in G$. Thus, $(a, a') \cdot (b, b') = (ab, a'b') \in G \times G'$.
- *Asscitivity*: We can obtain following using asscivity property of group G and G'.

  $((a, a') \cdot (b, b')) \cdot (c, c') = (ab, a'b') \cdot (c, c') = (abc, a'b'c') = (a, a') \cdot (bc, b'c') = (a, a') \cdot ((b, b') \cdot (c, c'))$

- *identity*: (1_G,1_{G'}) is the idenitity

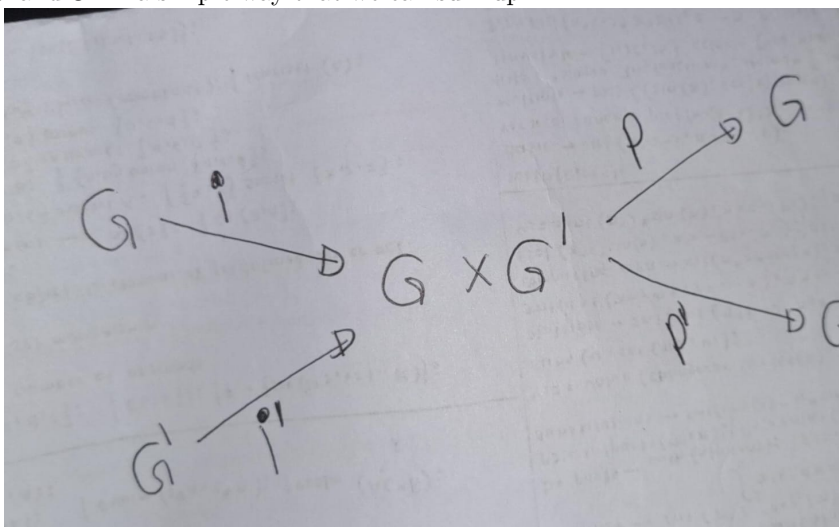
  $(1_G, 1_{G'}) \cdot (b, b') = (1_G b, 1_{G'} b') = (b, b') = (b 1_G, b' 1_{G'}) = (b, b') \cdot (1_G, 1_{G'})$

- *Inverse* : The inverse of (a, a') is $(a^{-1}, (a')^{-1})$

  $(a, a') \cdot (a^{-1}, (a')^{-1}) = (aa^{-1}, a'(a')^{-1}) = (1_G, 1_{G'}) = (a^{-1}a, (a')^{-1}a') = (a^{-1}, (a')^{-1}) \cdot (a, a')$

So, The group obtained in this way is called the product of G and G'.

It is related to the two factors G and G' in a simple way that we can sum up in terms of some homomorphisms.



The homomorphisms are defined as follows,

$$\begin{aligned} i : G &\rightarrow G \times G' && (12)\\ x &\mapsto (x, 1) && (13)\\ & && (14)\\ i' : G' &\rightarrow G \times G' && (15)\\ x &\mapsto (x', 1) && (16)\\ & && (17)\\ p : G \times G' &\rightarrow G' && (18)\\ (x, x') &\mapsto x && (19)\\ & && (20)\\ p' : G' \times G' &\rightarrow G' && (21)\\ (x, x') &\mapsto x' && (22)\\ & && (23)\\ & && (24) \end{aligned}$$

Observe that i and i' are injective and

$$Im(i) = G \times 1'_G \leq G \times G' \text{ and } Im(i') = 1_G \times G' \leq G \times G'$$

The maps p and p' are called projections and they are surjective.

$$\ker(p) = 1 \times G' \text{ and } \ker(p') = G \times 1_{G'}$$

It is obviously desirable to decompose a given group G as a product, that is, to find investigate groups H and H' such that G is isomorphic to the product $H \times H'$. The groups H and H' will be simpler, and the relation between $H \times H'$ and its factors is easily understood. It is rare that a group is a product, but it does happen occasionally

Consider a cyclicgroup of order 6 can be decomposed. It migheted be suprised you. A cyclic group C_6 of order 6 isisomorphic to the product $C_2 \times C_3$ of cyclic groups of orders 2 and 3.

$$C_6 \equiv C_2 \times C_3$$

Let say

$$\begin{aligned} C_2 &= < y >= \{1, y\}, \text{ with } y^2 = 1 && (25)\\ C_3 &= < z >= \{1, z, z^2\}, \text{ with } y^3 = 1 && (26) \end{aligned}$$

Let $x \in C_2 \times c_3$. Then there exist $p \in C_2$ and $q \in C_3$ such that $x = (p, q)$. Let's find order of x, that is the smallest positive integer k such that $x^k = (y^k, z^k)$ is the identity $(1, 1)$.

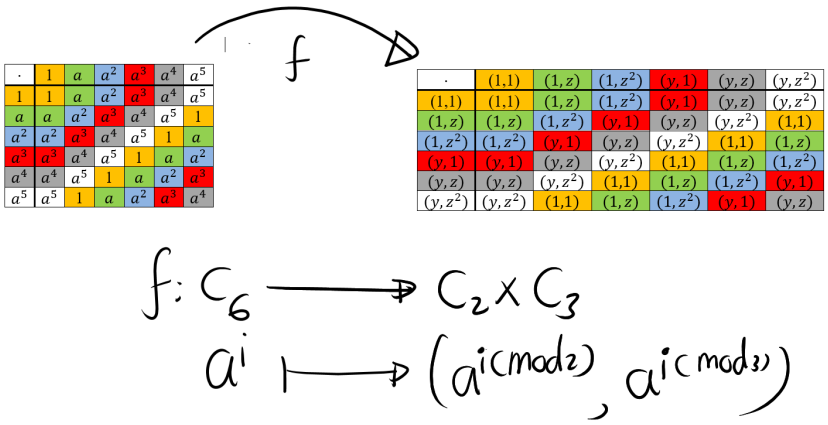
- *Case-I*: $k = 1, x^1 = (y^1, z^1) = (y, z)$
- *Case-II*: $k = 2, x^2 = (y^2, z^2) = (1, z^2)$
- *Case-III*: $k = 3, x^3 = (y^3, z^3) = (y, 1)$
- *Case-IV*: $k = 4, x^4 = (y^4, z^4) = (1, z)$
- *Case-V*: $k = 5, x^5 = (y^5, z^5) = (1, z^2)$
- *Case-VI*: $k = 6, x^5 = (y^6, z^6) = (1, 1)$

Thus, the smallest positive integer k such that $x^k = (1, 1)$ is 6. So, order of x is 6. Since $C_2 \times C_3$ has order 6. Furthur,

$$C_2 \times C_3 =< x >$$

The powers of x are

$$(1, 1), (y, z), (1, z^2), (y, 1), (1, z), (y, z^2)$$



Here $i = 0, 1, 2...5$

So let's try to see above result more generally.

Let r and s be relatively prime integers. A cyclic group of order rs is isomorphic to the product of a cyclic group of order r and a cyclic group of order s.

On the other hand, a cyclic group of order 4 is not isomorphic to a product of two cyclic groups of order 2.

$$C_4 \not\equiv C2 \times C_2$$

Because , every element of $C_2 \times C_2$ has order 1 or 2,whereasa cyclic group of order 4 contains two elements of order 4.

The next proposition describes product groups.

Let G be a group and let $H, K \leq G$, and let $f : H \times K \to G$ be the multiplication map, defined by $f(h, k) = hk$. Its image is the set $HK = \{hk | h \in H, k \in K\}$.

a. f is injective if and only if $H \cap K = \{1\}$.
b. f is a homomorphism from the product group $H \times K$ to G if and only if elements of K commute with elements of H: $hk = kh$.
c. If H is a normal subgroup of G, then HK is a subgroup of G.
d. f is an isomorphism from the product group $H \times K$ to G if and only if $H \cap K = \{1\}$, $HK = G$, and also H and K are normal subgroups of G.

It is important to note that the multiplication map may be bijective though it isn't a group homomorphism. This happens, for instance, when $G = S_3$, and with the usual notation, $H = \langle x \rangle$ and $K = \langle y \rangle$.

a.

- ($\Longrightarrow$) We are going to use proof by contrapositive. So, suppose that $x \in H \cap K$ such that $x \neq 1$. Since $x \in H$ then $x^{-1} \in H$.

$$f(x^{-1}, x) = x^{-1} \cdot x = 1 = 1 \cdot 1 = f(1, 1)$$

Thus, f is not injective. Thus, if f is injective then $H \cap K = \{1\}$. -($\Longleftarrow$) Now Suppose that $H \cap K = \{1\}$. Let $(h_1, k_1), (h_2, k_2) \in H \times K$ such that $h_1 k_1 = h_2 k_2$. Now multiply both sides of this equation on the left by h_1^{-1} and on the right by k_2^{-1},

$$\begin{aligned} h_1 k_1 &= h_2 k_2 && (27)\\ h_1^{-1}(h_1 k_1)k_2^{-1} &= h_1^{-1}(h_2 k_2)k_2^{-1} && (28)\\ (h_1^{-1}h_1)k_1 k_2^{-1} &= h_1^{-1}h_2(k_2 k_2^{-1}) && (29)\\ k_1 k_2^{-1} &= h_1^{-1}h_2 && (30) \end{aligned}$$

Note that $(k_1 k_2^{-1}) \in K$ and $h_1^{-1}h_2 \in H$. Since $H \cap K = \{1\}$,

$$k_1 k_2^{-1} = h_1^{-1}h_2 = 1$$

. Then,

$$k_1 = k_2 \quad \text{and} \quad h_1 = h_2.$$

Then

$$(h_1, k_1) = (h_2, k_2)$$

b. Let $(h_1, k_1), (h_2, k_2) \in H \times K$. Now consider,

$$\begin{aligned} f((h_1, k_1) \cdot (h_2, k_2)) &= f((h_1 h_2, k_1 k_2)) = h_1 h_2 k_1 k_2 && (31)\\ f((h_1, k_1)) \cdot f((h_2, k_2)) &= (h_1 k_1) \cdot (h_2 k_2) = h_1 k_1 h_2 k_2 && (32) \end{aligned}$$

$$
\begin{aligned}
f \text{ is homorphism} &\iff f((h_1,k_1)\cdot(h_2,k_2)) = f((h_1,k_1))\cdot f((h_2,k_2)) && (33)\\
&\iff h_1h_2k_1k_2 = h_1k_1h_2k_2 && (34)\\
&\iff h_1^{-1}(h_1h_2k_1k_2)k_2^{-1} = h_1^{-1}(h_1k_1h_2k_2)k_2^{-1} && (35)\\
&\iff (h_1^{-1}h_1)h_2k_1(k_2k_2^{-1}) = (h_1^{-1}h_1)k_1h_2(k_2k_2^{-1}) && (36)\\
&\iff (h_1^{-1}h_1)h_2k_1(k_2k_2^{-1}) = (h_1^{-1}h_1)k_1h_2(k_2k_2^{-1}) && (37)\\
&\iff h_2k_1 = k_1h_2 && (38)
\end{aligned}
$$

c.

- Suppose that H is a normal sub group of G. Note that

$$KH = \bigcup_{k\in K} kH \quad \text{and} \quad HK = \bigcup_{k\in K} Hk$$

Since, H is normal, $kH = Hk$ for all $k \in K$. So, $HK = KH$. We are going to use sub group test,

  - *non-emptyness*: Clearly, $1 = 1 \cdot 1 \in HK$ (because $1 \in H$ and $1 \in K$
  - *closure*:
$$HKHK = HHKK = HK$$
Thus, HK is closed under multiplication.
  - *closed under inverse*: Let $hk \in HK$. Then
$$(hk)^{-1} = k^{-1}\cdot h^{-1} \in KH = HK$$
This proves closure of HK under inverses.

d.

- ($\Longleftarrow$): Suppose that $H \cap K = \{1\}$, $HK = G$, and also $H, K \trianglelefteq G$. According to the (b), f is a homomorphism from $H \times K$ to G if and only if $hk = kh$ for all $h \in H$. Consider,

$$(hkh^{-1})k^{-1} = h(kh^{-1}k^{-1}).$$

Note that, Since $K \trianglelefteq G$, $hkh^{-1} \in K$. So,$(hkh^{-1})k^{-1} \in K$. Similary we can show that $h(kh^{-1}k^{-1}) \in H$.Thus,

$$(hkh^{-1})k^{-1} = h(kh^{-1}k^{-1}) \in H \cap K.$$

But from our hypothesis, $H \cap K = \{1\}$. Hence,

$$hkh^{-1}k^{-1} = 1 \quad (39)$$
$$hk = kh \quad (40)$$

Therefore, by (b) we can f is hormorphism. Now we have to proove bijectivity, - *Injectivity*: Already prooved in @ref(prp:prp2114) (a) - *Surjectivity*: For any $g \in G$, we can write $g = hk$ for some $h \in H$ and $k \in K$ (since $Im(f) = HK = G$). Thus, $f(h, k) = hk = g$, so f is surjective.

Therefore f is an isomorphism.

- ($\Longrightarrow$) Now suppose that f is isomorphism.
  - **Claim i**: $H \cap K = \{1\}$.
    Suppose that $x \in H \cap K$. Then,
    $$f(1, x) = x = f(x, 1)$$
    Since f is an isomorphism (and hence injective), we must have $x = 1$. Therefore, $H \cap K = \{1\}$.
  - **Claim ii** :$HK = G$.
    Since f is surjective, for any $g \in G$, there exist $h \in H$ and $k \in K$ such that $f(h, k) = hk = g$. Therefore, $HK = G$.
  - **Claim iii** : H and K are normal in G.
    For any $h \in H$ and $g \in G$, we can write $g = hk$ for some $k \in K$. Then
    $$ghg^{-1} = (hk)h(hk)^{-1} = hk(hh^{-1})k^{-1} = h(kk^{-1}) = h \in H.$$
    Thus, $H \trianglelefteq G$. Similarly, we can show that $K \trianglelefteq G$.

There are two isomorphism classes of groups of order 4, the class of the cyclic group C_4 of order 4 and the class of the Klein Four Group,which is isomorphic to the product $C_2 \times C_2$ of two groups of order 2.

Let G be a group of order 4. The order of any element x of G divides 4, so there are two cases to consider:

- Case 1: G contains an element of order 4($|G| = 4$). Then G is a cyclic group of order 4.
- Case 2: Every element of G except the identity has order 2.
  In this case, $x = x^{-1}$ for every element x of G. Let x and y be two elements of G. Then xy has order 2, so $(xy)(x^{-1}y^{-1}) = (xy)(xy) = 1$. This shows that x and y commute,

$$\begin{aligned} xyx^{-1}y^{-1} &= 1 && (41)\\ xyx^{-1}(y^{-1}y) &= y && (42)\\ xyx^{-1} &= y && (43)\\ xy(x^{-1}x) &= yx && (44)\\ xy &= yx && (45) \end{aligned}$$

since x, y are arbitrary elements, G is abelian. So every subgroup is normal. We choose distinct elements x and y in G, and we let H and K be the cyclic groups of order 2 that they generate. Proposition @ref(prp:prp2114) (d) shows that G is isomorphic to the product group $H \times K$.

Quotient Groups

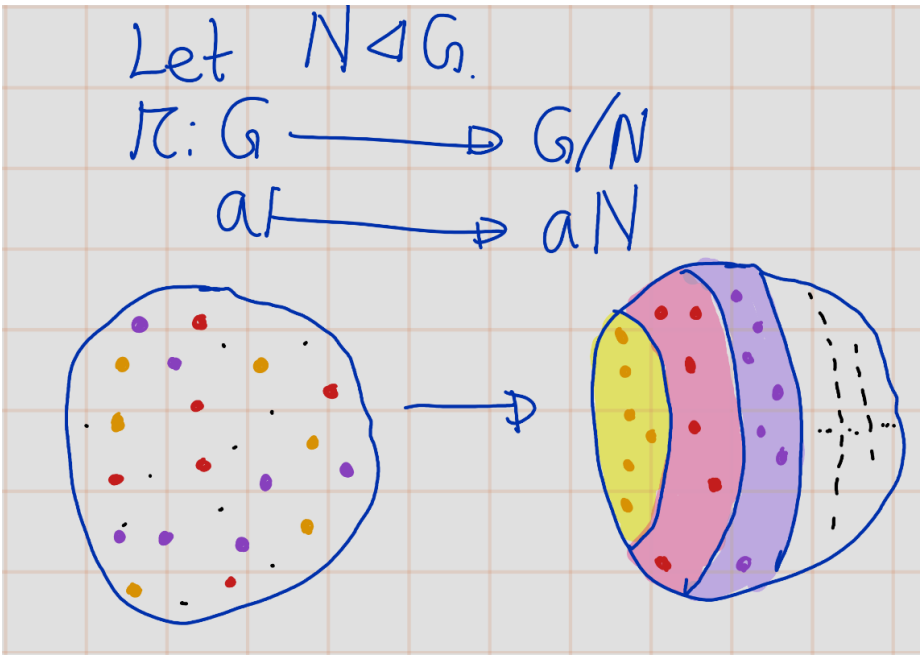
The set of cosets of a normal subgroup N of a group G is often denoted by G/N.

$$G/N \text{ is the set of cosets of } N \text{ in} G$$

Notation: When we regard a coset C as an element of the set of cosets, the bracket notation $[C]$ may be used. If $C = aN$, we may also use the bar notation to denote the element $[C]$ by $\overline{a}$, and then we would denote the set of cosets by $\overline{G}$:

$$\overline{G} = G/N$$

Let N be a normal subgroup of a group G, and let G denote the set of cosets of N in G. There is a law of composition on G that makes this set into a group, such that the map $\pi : G \to \overline{G}$ defined by $\pi(a) = \overline{a}$ is a surjective homomorphism whose kernel is N.



The map is often referred to as the canonical map from G to $\overline{G}$. The word "**canonical**" indicates that this is the only map that we might reasonably be talking about

The next corollary is very simple, but it is important enough to single out:

Let $N \trianglelefteq G$, and let $\overline{G}$ denote the set of cosets of N in G. Let $\pi : G \to \overline{G} = G/N$ be the canonical homomorphism. Let $a_1, \ldots, a_k \in G$ such that the product $a_1 \cdots a_k \in N$. Then $\overline{a_1} \cdots \overline{a_k} = \overline{1}$.

Let $p = a_1 \cdots a_k \in N$. This implies $\pi(p) = \overline{p} = \overline{1}$.
Since is pi a homomorphism, $\pi(p) = \pi(a_1 \cdots a_k) = \pi(a_1) \cdots \pi(a_k) = \overline{a_1} \cdots \overline{a_n}$

Proof of @ref(thm:2122) There are several things to be done. We must

- define a law of composition on $\overline{G}$,
- prove that the law makes $\overline{G}$ into a group,
- prove that π is a surjective homomorphism, and
- prove that the kernel of π is N.

If $A, B \subseteq G$ then AB denotes the set of products ab:

$$AB := \{x \in G : x = ab, a \in A, b \in B\}$$

- We will call this a product set, though in some other contexts the phrase "product set" refers to the set $A \times B$ of pairs of elements

Let N be a normal subgroup of a group G, and let aN and bN be cosets of N. The product set $(aN)(bN)$ is also a coset and

$$(aN)(bN) = \{x \in G : x = anbn' \ \& \ n, n' \in N\} = abN$$

.

Since N is a subgroup, $NN = N$.
Since N is normal, left and right cosets are equal: $Nb = bN$.

$$(aN)(bN) = a(Nb)N = a(bN)N = abNN = abN$$

- This lemma allows us to define multiplication on the set $\overline{G} = G/N$.
- Using the bracket notation, the definition is this: If C_1 and C_2 are cosets, then $[C_1][C_2] = [C_1C_2]$, Where C_1C_2 is the product set.
- The lemma shows that this product set is another coset.

- To compute the product $[C_1][C_2]$, take any elements $a \in C_1$ and $b \in C_2$. Then $C_1 = aN$, $C_2 = bN$, and C_1C_2 is the coset abN that contains ab. So,

  $$[aN][bN] = [abN] \text{ or } \overline{a}\overline{b} = \overline{ab}.$$

  Then by definition of the map π in theorm @ref(thm:2122),

  $$\pi(ab) = \overline{a}\overline{b} = \overline{ab} = \pi(a)\pi(b)$$

  The fact that π is a homomorphism will follow, once we show that G is a group. Since the canonical map π is surjective , the next lemma proves this

Let G be a group, and let Y be a set with a law of composition (both laws written with multiplicative notation). Consider a surjective map $\varphi : G \to Y$ with the homomorphism property: $\varphi(ab) = \varphi(a)\varphi(b)$ for all a and b in G. Then Y is a group, and φ is a homomorphism.

The group axioms that are true in G are carried over to Y by the surjective map φ.

- **Closure** : Let $y_1, y_2 \in Y$. Since φ is surjective, $y_1 = \varphi(x_1), y_2 = \varphi(x_2)$ for some $x_1, x_2 \in G$.

  $$y_1y_2 = \varphi(x_1)\varphi(x_2) = \varphi(x_1x_2) \in Y$$

- **Assciativity Property** :
  Let y_1, y_2, and y_3 be elements of Y. Since φ is surjective, $y_i = \varphi(x_i)$ for some x_i in G. Then

$$(y_1y_2)y_3 = (\varphi(x_1)\varphi(x_2))\varphi(x_3) = \varphi(x_1x_2)\varphi(x_3) = \varphi((x_1x_2)x_3) \quad (46)$$
$$=^* \varphi(x_1(x_2x_3)) = \varphi(x_1)\varphi(x_2x_3) = y_1(y_2y_3) \quad (47)$$

The equality marked with an asterisk ($=^*$) is the associative law in G. The other equalities follow from the homomorphism property of φ.

- **Identity** Let $y \in Y$. Since φ is surjective, there exist $x \in G$ such that $y = \varphi(x)$. Let 1_G be identity of G Then,

  $y\varphi(1_G) = \varphi(x)\varphi(1_G) = \varphi(x1_G) = \varphi(x) = y = \varphi(1_Gx) = \varphi(1_G)\varphi(x) = \varphi(1_G)y$

  Thus, $\varphi(1_G)$ is the identity of Y.

- **Inverse** : Let $y \in G$. Since φ is surjective, there exist $x \in G$ such that $y = \varphi(x)$,

  $y\varphi(x^{-1} = \varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(1_G) = \varphi(x^{-1}x) = \varphi(x^{-1})\varphi(x) = \varphi(x^{-1})y$

  Thus, $y^{-1} = \varphi(x)$

The only thing remaining to be verified is that the kernel of the homomorphism π is the subgroup N.

$$\pi(a) = \pi(1) \iff \bar{a} = \bar{1} \quad (48)$$
$$\iff [aN] = [1N] \quad (49)$$
$$\iff a \in N. \quad (50)$$

Thus, $\ker(\pi) = N$

Our assumption that N is a **normal** subgroup of G is crucial to lemma @ref(lem:2125). If H is **not** normal, there will be left cosets C_1 and C_2 of H in G such that the product set C_1C_2 does not lie in a single left cosets.

Let's see an example for this. Going back once more to the subgroup $H = \langle y \rangle$ of S_3. Note that the subgroup H is not normal.
The product set $(1H)(xH)$ contains four elements:

$$(1H)(xH) = \{1, y\}\{x, xy\} = \{x, xy, x^2y, x^2\}$$

. It is not a coset.

The next theorem relates the quotient group construction to a general group homomorphism, and it provides a fundamental method of identifying quotient groups.

Let $\varphi : G \to G'$ be a surjective group homomorphism with kernel N. The quotient group $\overline{G} = G/N$ is isomorphic to the image G'. To be precise, let $\pi : G \to \overline{G} = G/N$ be the canonical map. There exists a unique isomorphism $\overline{\varphi} : G/N \to G'$ such that $\varphi = \psi \circ \pi$.

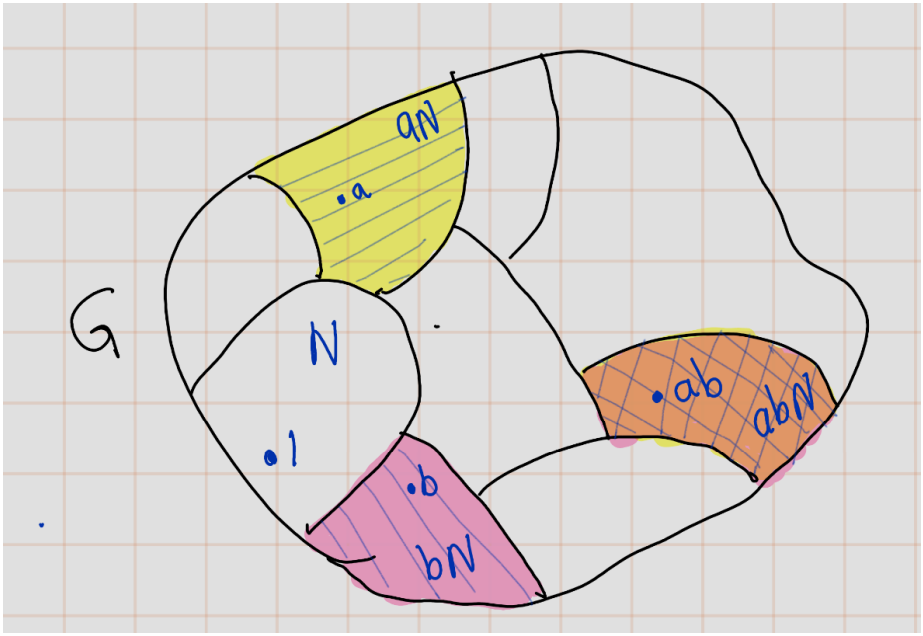
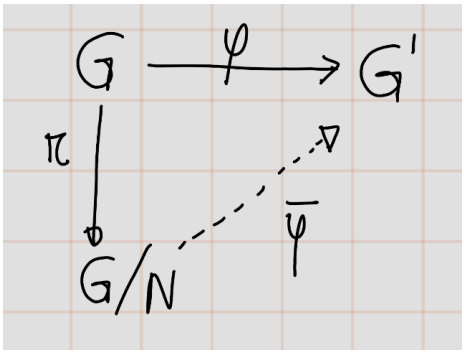


Figure 2: A Schematic Diagram of Coset Multiplication.



The elements of $\overline{G} = G/N$ are the cosets of N, and they are also the fibres of the map φ. The map $\overline{\varphi}$ referred to in the theorem is the one that sends a non-empty fibre to its image: $\overline{\varphi}(\overline{x}) = \varphi(x)$. For any surjective map of sets $\varphi : G \to G'$, one can form the set $\overline{G}$ of fibres, and then one obtains a diagram as above, in which $\overline{\phi}$ is the bijective map that sends a fibre to its image. When ϕ is a group homomorphism, $\overline{\phi}$ is an isomorphism because

$$\overline{\phi}(\overline{ab}) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}(\overline{a})\overline{\phi}(\overline{b}).$$

Let $\varphi : G \to G'$ be a group homomorphism with kernel N and image H'. The quotient group $\overline{G} = G/N$ is isomorphic to the image H'.

Lienaer Operators

Exercises

Chapter 2

Laws of composition

Let S be a set. Prove that the law of composition defined by $ab = a$ for all a and b in S is associative? For which sets does this law have an identity?

Solution: Let $a, b, c \in S$. Now consider following

$$(ab)c = (ac) = a = (ab) = a(bc)$$

Thus, the given law of composition is associative.

If the given law of composition has an identity element whenever every element $a \in S$ has a multiplicative inverse./ In other words, for every element $a \in S$, there exists an element $e \in S$ such that

$$ae = ea = a.$$

Thus, $ae = a = ea = e$. So, the identity element is the same as every element in S, and the law has an identity for all sets S. Thus, only singletons sets have this given law of compositions have identity.

Prove the properties of inversesthat are listed near the end ofthe section.

- If an element a has both a left inverse l and a right inverse r, then $r = l$, a is invertible and r is its inverse.

Since l is a left inverse for a, then $la = 1$. In the same way, since r is a right inverse for a the equality $ar = 1$ holds. Let us now consider the expression lar. By associativity of the composition law in a group we have $r = 1r = (la)r = lar = l(ar) = l1 = l$. This implies that $l = r$. Since $l = r$, it holds also that that $ar = 1 = la = ra$ hence a is invertible and r is its inverse.

- If a is invertible, its inverse is unique.

Let i_1 and i_2 be inverses of a. In particular i_1 is a left inverse of a and i_2 is a right inverse of a. By point (a) $i_1 = i_2$.

- Inverses multiply in the opposite order: if a and b are invertible, then the product ab is invertible and $(ab)^{-1} = b^{-1}a^{-1}$.

In order to show that ab is invertible, it is enough to exhibit an element that is a right and a left inverse of ab. The element $b^{-1}a^{-1}$ is a right inverse of ab since $abb^{-1}a^{-1} = a(bb^{-1})a^{-1} = a1a^{-1} = aa^{-1} = 1$. It is a left inverse since $b^{-1}a^{-1}ab = b^{-1}(a^{-1}a)b = b^{-11}b = b^{-1}b = 1$. This proves that ab is invertible and that $b^{-1}a^{-1}$ is its inverse.

Groups and Subgroups

Make a multiplication table for the symmetric group S_3.

Solution

$\circ$	**e**	(12)	(13)	(23)	(123)	(132)
e	e	(12)	(13)	(23)	(123)	(132)
(12)	(12)	e	(123)	(132)	(13)	(23)
(13)	(13)	(123)	e	(132)	(23)	(12)
(23)	(23)	(132)	(123)	e	(12)	(13)
(123)	(123)	(13)	(23)	(12)	(132)	e
(132)	(132)	(23)	(12)	(13)	e	(123)

Let S be a se t with an associative law of composition and with an identity element. Prove that the subset consisting of the invertible elements in S is a group.

Let $S^* \subseteq S$ with consisting of the invertible elements in S.

- *identity* : We are given identity element $1 \in S$ and $(1^{-1})(1) = 1 \implies 1 \in S^*$.
- *Closure* : So let $a, b \in S^*$. Then a, b are invertible. Let $a^{-1}, b^{-1} \in S^*$ be inverses of a and b respectively. Now we need to check $ab \in S^*$.

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = e = aa^{-1} = a(bb^{-1})a^{-1} = (ab)(b^{-1}a^{-1})$$

Thus, $(ab)^{-1} = b^{-1}a^{-1}$. So, $ab \in S^*$ Therefore, S^* is closed under the composition.

- *Associativity*: The associativity property inherit from the group S.

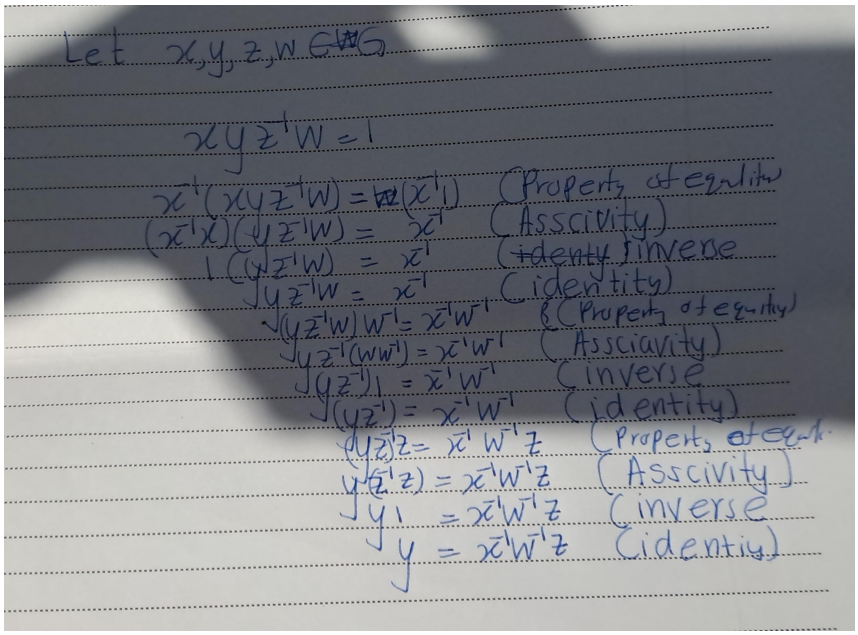
Therefore, S^* is a group.

Let G be a group.Let $x, y, z, w \in G$.

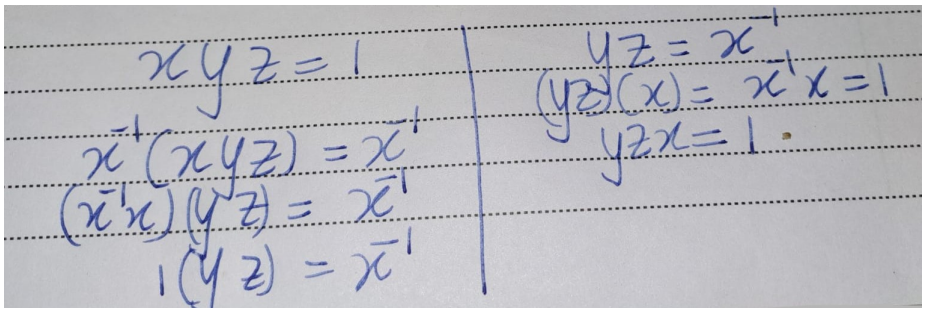
(a) Solve for y, given that $xyz^{-1}w = 1$.
(b) Suppose that $xyz = 1$. Does it follow that $yzx = 1$? Does it follow that $yxz = 1$?

Solution:

a.



b.



- The given statement is false.

$$\begin{aligned} xyz &= 1 && (51)\\ x^{-1}(xyz) &= x^{-1}\cdot 1 && (52)\\ (x^{-1}x)(yz) &= x^{-1} && (53)\\ 1\cdot(yz) &= x^{-1} && (54)\\ (yz) &= x^{-1} && (55)\\ (yz)z^{-1} &= x^{-1}z^{-1} && (56)\\ y(zz^{-1}) &= x^{-1}z^{-1} && (57)\\ y\cdot 1 &= x^{-1}z^{-1} && (58)\\ yx &= x^{-1}z^{-1}x && (59)\\ yxz &= x^{-1}z^{-1}xz && (60)\\ & && (61) \end{aligned}$$

If G is not abelian or $z \neq x$. $xyz = 1 \nRightarrow yxz = 1$.

In which of the following cases is H a subgroup of G?

(a) $G = GL_n(\mathbb{C})$ and $H = GL_n(\mathbb{R})$.

(b) $G = \mathbb{R}^\times$ and $H = \{1, -1\}$.

(c) $G = \mathbb{Z}^+$ and H is the set of positive integers.

(d) $G = \mathbb{R}^+$ and H is the set of positive reals.

(e) $G = GL_2(\mathbb{R})$ and H is the set of matrices $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ with all entries equal to 0.

Solution:

(a)

- *Subset ?* : Since every matrix with real entries can be interpreted as a matrix with complex entries, we conclude that $H \subset G$.
- *Closure ?* : For every $A, B \in GL_n(\mathbb{R})$ we have $AB \in GL_n(\mathbb{R})$ since Product of invertible matrices is invertible. I proved this result in chapter 1.
- *Identity ?* :The identity in G is I_n, the identity nxn matrix. Observe that $I_n \in H = GL_n(\mathbb{R})$. (Because every entry of I_n is 1 or 0)

- *Inverse ?*: $GL_n(\mathbb{R})$ is the set of $n \times n$ invertible matrices with real entries. So, all the elements in H is invertible.

Therefore, $H \leq G$

(b)

- *Subset ?* : This is trivial $\{-1, 1\} \subset \mathbb{R}^\times$
- *Closure ?* :

$$\begin{aligned} 1 \times 1 &= 1 \in H && (62)\\ (-1) \times 1 &= (-1) \in H && (63)\\ 1 \times (-1) &= (-1) \in H && (64)\\ (-1) \times (-1) &= -1 \in H && (65)\\ & && (66) \end{aligned}$$

Thus, H is closed. - *Identity ?* : The identity in G is 1, which is also in H.

- *Inverse ?* :

$$\begin{aligned} 1 \times 1 = 1 &\implies (1)^{-1} = 1 \in H && (67)\\ (-1) \times (-1) = 1 &\implies (-1)^{-1} = (-1) \in H && (68) \end{aligned}$$

x'Therefore, H is sub group of G.

(c) Note that $2 \in H$, but inverse of 2 in $\mathbb{Z}^+$ is $(-2) \notin H$.
Therefore, H is not a subgroup of G.

(d)

- *Subset ?* : This is trivial. $H \subset \mathbb{R}^\times$
- *Closure ?* : Product of positive real number is positive. Thus, H is closed.
- *Identity ?* : 1 is the identity of G, which is in H.
- *Inverse ?* : Let $a \in H$. Then,

$$a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$$

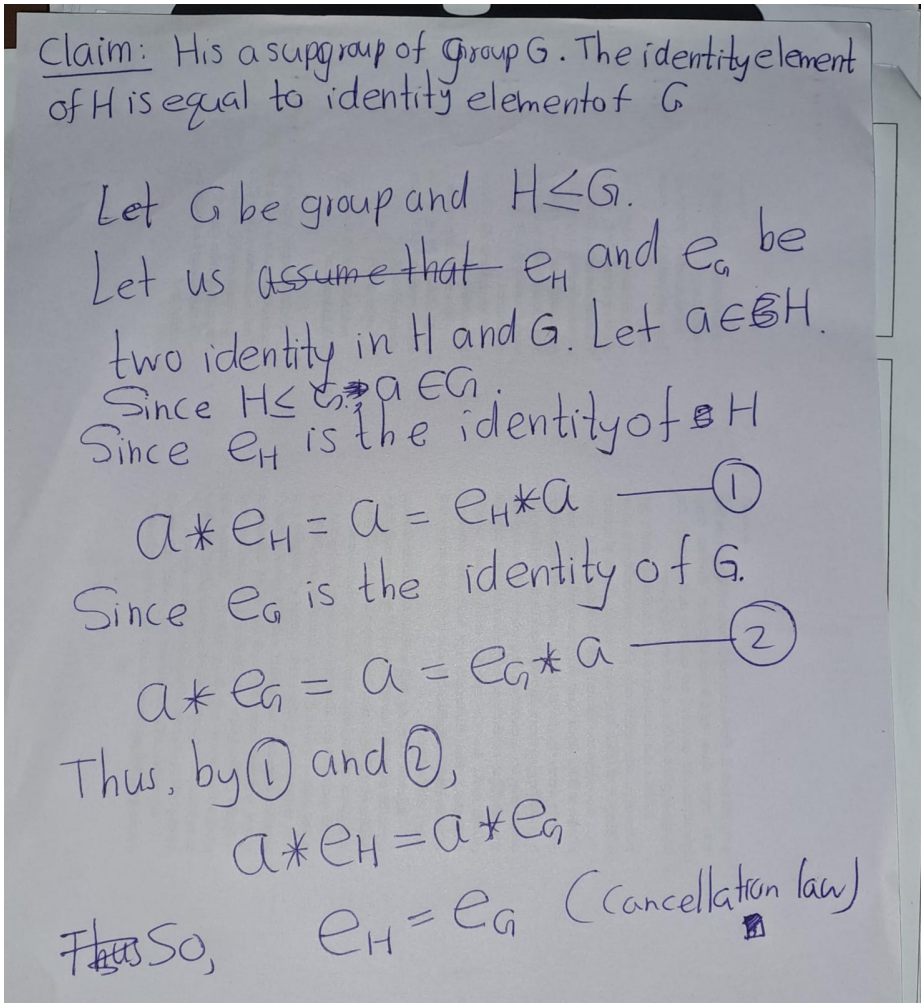
So, $\frac{1}{a} \in H$ is the inverse of a. Thus, H is closed under inverses.

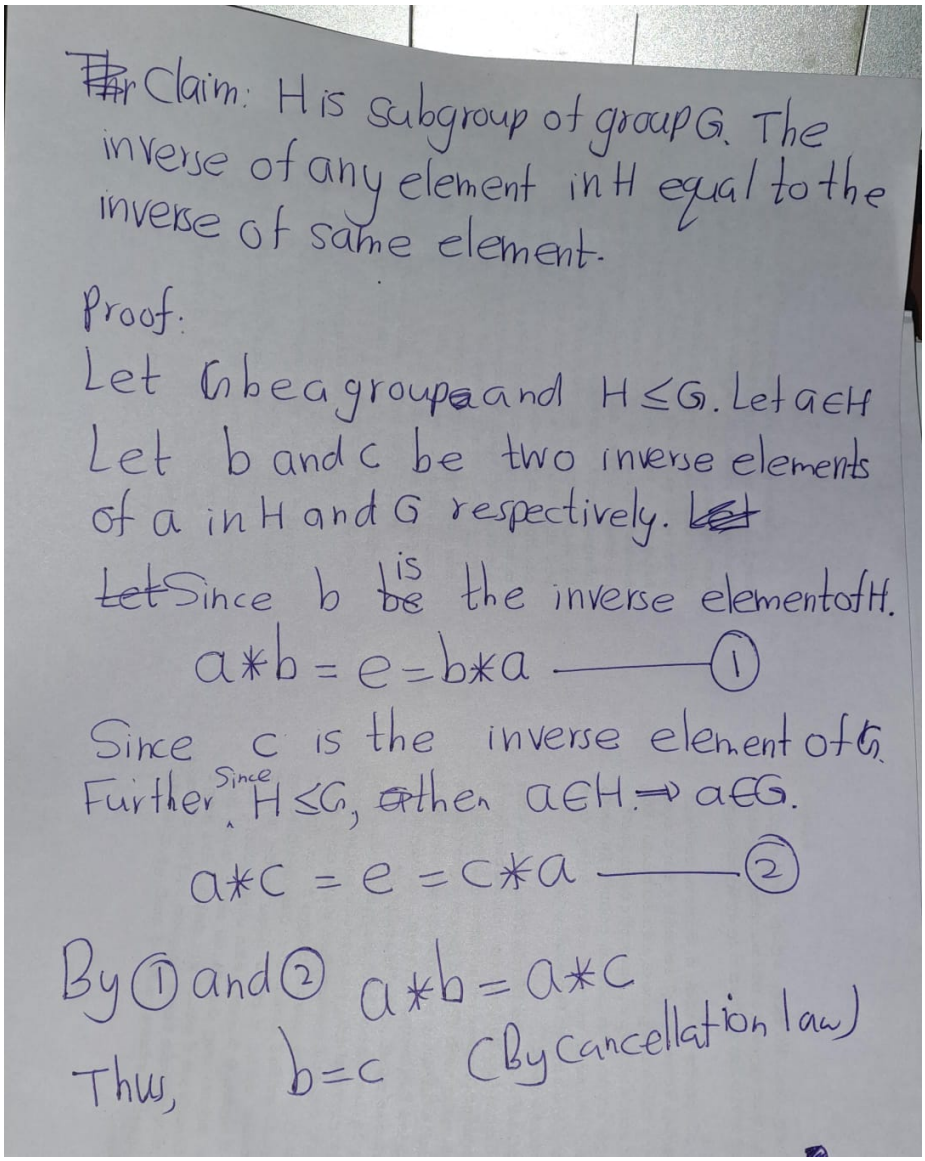
(e) Let $A = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}$ Then $A \in H$. But observe that $det(A) = 0 \implies A$ is not invertible. Thus, $A \notin H$. Thus, this $H \not\subseteq G$.

Therefore, H is not a subgroup of G.

In the definition of a subgroup, the identity element in H is required to be the identity of G. One might require only that H have an identity element, not that it need be the same as the identity in G.

- Show that if H has an identity at all, then it is the identity in G.
- Show that the analogous statement is true for inverses.

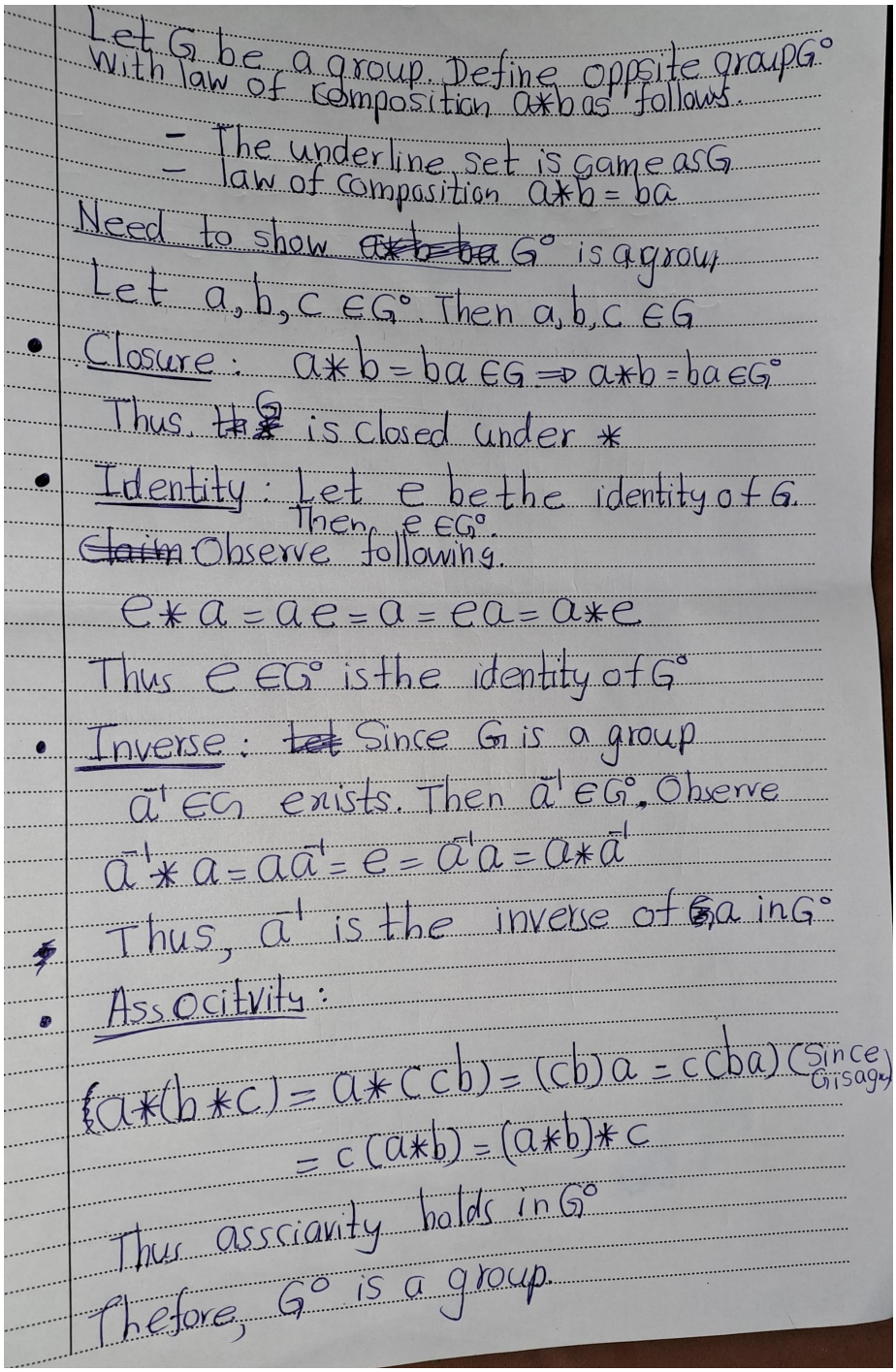




Let G be a group. We define an opposite group G° with the law of composition $a*b$ as follows: - The underlying set is the same as G, - but the law of composition is $a * b = ba$.

Prove that G° is a group.

Solution:



Let G be a group. Define opposite group G° with law of composition $a*b$ as follows.

- The underline set is same as G
- law of composition $a*b = ba$

Need to show ~~$a*b = ba$~~ G° is a group

Let $a, b, c \in G^\circ$. Then $a, b, c \in G$

- Closure: $a*b = ba \in G \Rightarrow a*b = ba \in G^\circ$

  Thus, ~~$*$~~ G is closed under $*$

- Identity: Let e be the identity of G. Then, $e \in G^\circ$.

  ~~Claim~~ Observe following.

  $e*a = ae = a = ea = a*e$

  Thus $e \in G^\circ$ is the identity of G°

- Inverse: ~~let~~ Since G is a group $\bar{a}^1 \in G$ exists. Then $\bar{a}^1 \in G^\circ$. Observe

  $\bar{a}^1 * a = a\bar{a}^1 = e = \bar{a}^1 a = a * \bar{a}^1$

  Thus, $\bar{a}^1$ is the inverse of ~~G~~ a in G°

- Associtivity:

  $(a*(b*c) = a*(cb) = (cb)a = c(ba)$ (Since G is a group)

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

Thus asscianity holds in G°

Thefore, G° is a group.

Subgroups of the Additive Group of Integers

Let $a = 123$ and $b = 321$. Compute $d = gcd(a, b)$, and express d as an integer combination $ra + bs$.

Solution:

We use Euclidean Algorithm

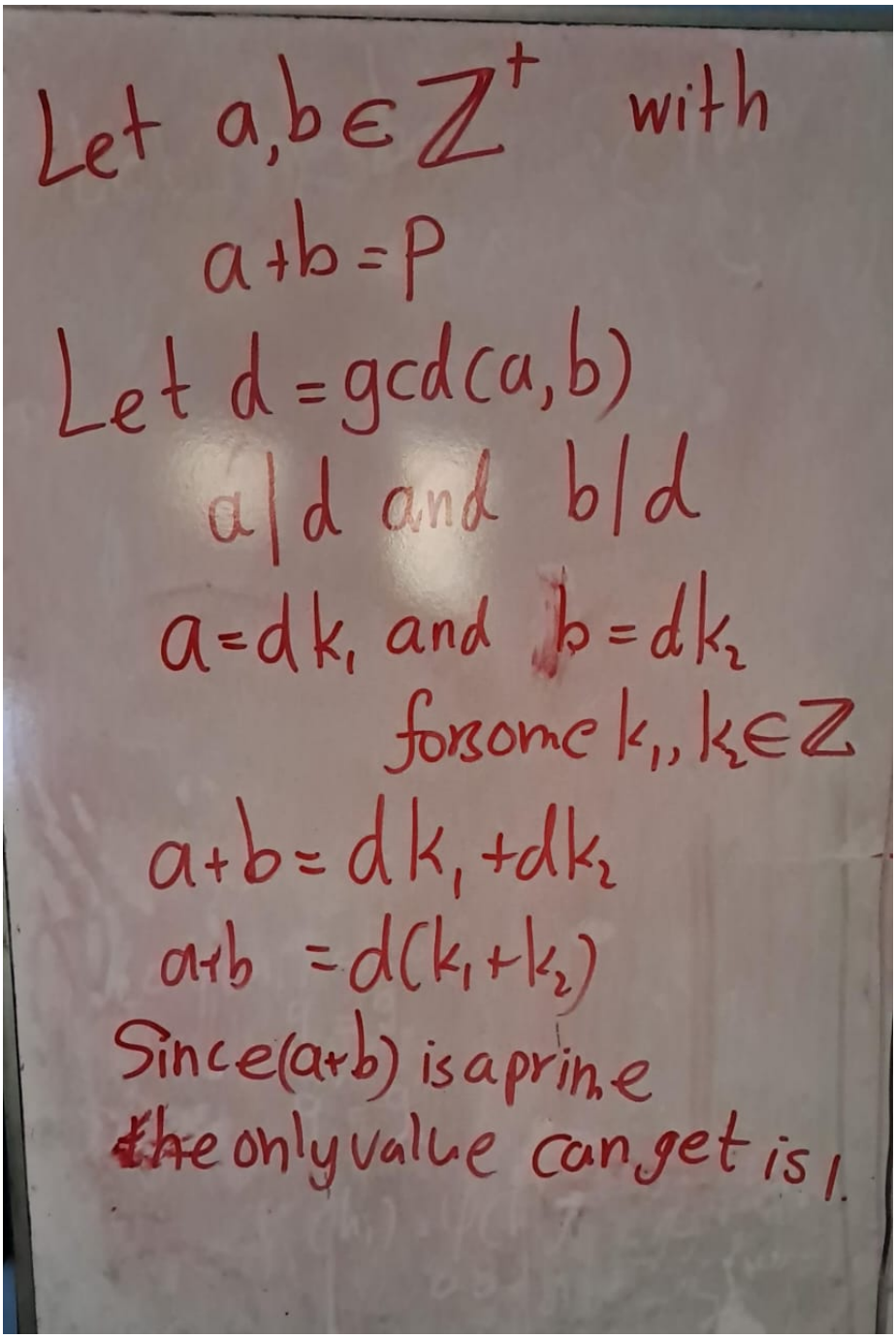
$321 = 2(123) + 75$
$123 = 1(75) + 48$
$75 = 1(48) + 27$
$48 = 1(27) + 21$
$27 = 1(21) + 6$
$21 = 3(6) + 3$
$6 = 2(3) + 0$

Thus $gcd(123, 321) = 3$.
Now let's backsubstute it.

$3 = 21 - 3(6)$
$= 1(21) - 3(27 - 1(21))$
$= 1(21) - 3(27) + 3(21)$
$= 4(21) - 3(27)$
$= 4(48 - 1(27)) - 3(27)$
$= 4(48) - 7(27)$
$= 4(48) - 7(75 - 1(48))$
$= 11(48) - 7(75)$
$= 11(123 - 1(75)) - 7(75)$
$= 11(123) - 18(75)$
$= 11(123) - 18(321 - 2(123))$
$= 47(123) - 18(321)$

Prove that if a and b are positive integers whose sum is a prime p, their greatest common divisor is 1.

Solution:

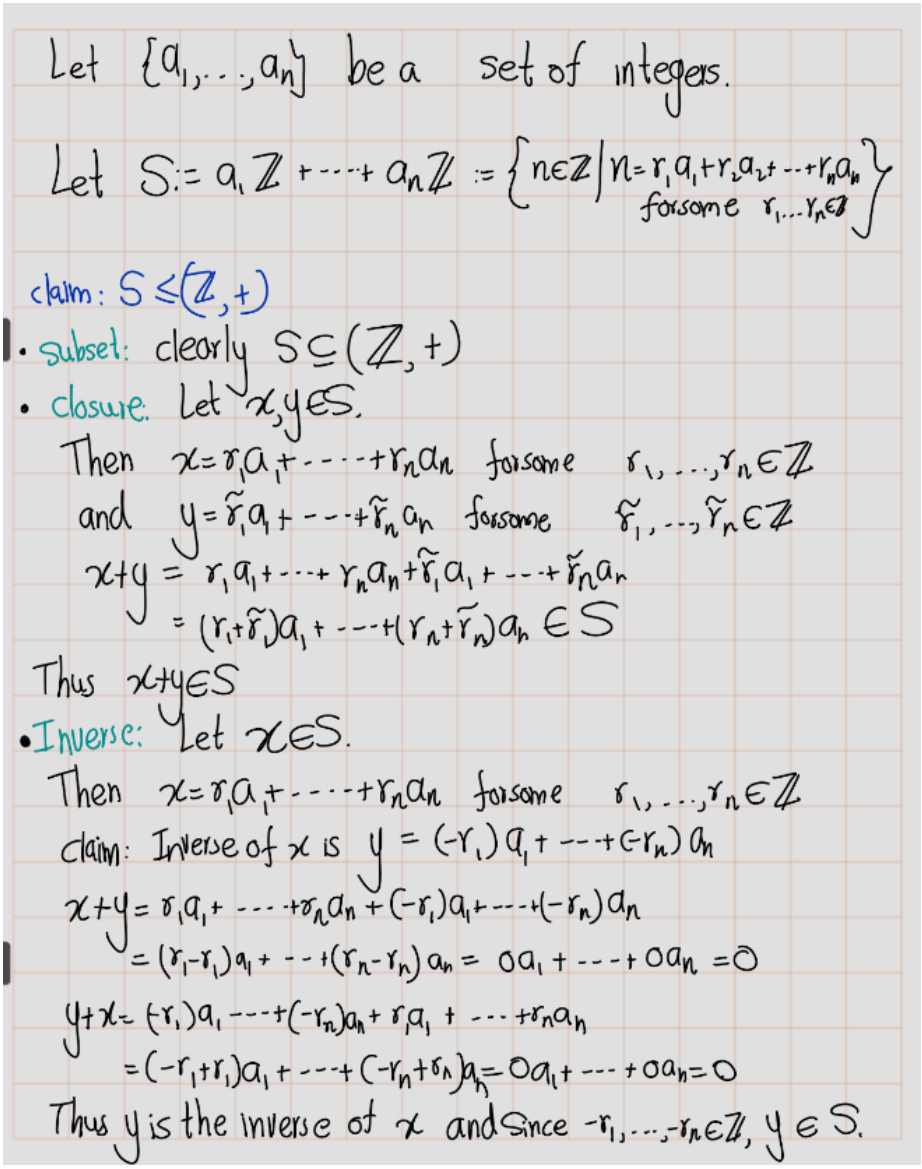


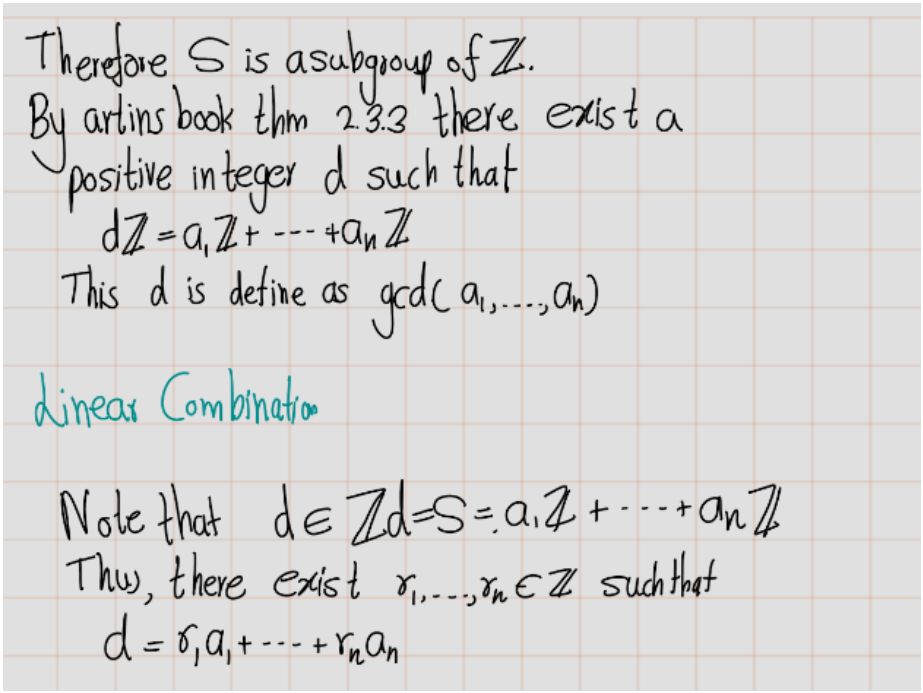
a. Define the greatest common divisor of a set $\{a_1, ..., a_n\}$ of n integers. Prove that it exists, and that it is an integer combination of $a_1, ..., a_n$.

b. Prove that if the greatest common divisor of $\{a_1, ..., a_n\}$ is d, then the greatest common divisor of $\{a_1/d, ..., a_n/d)$ is 1.

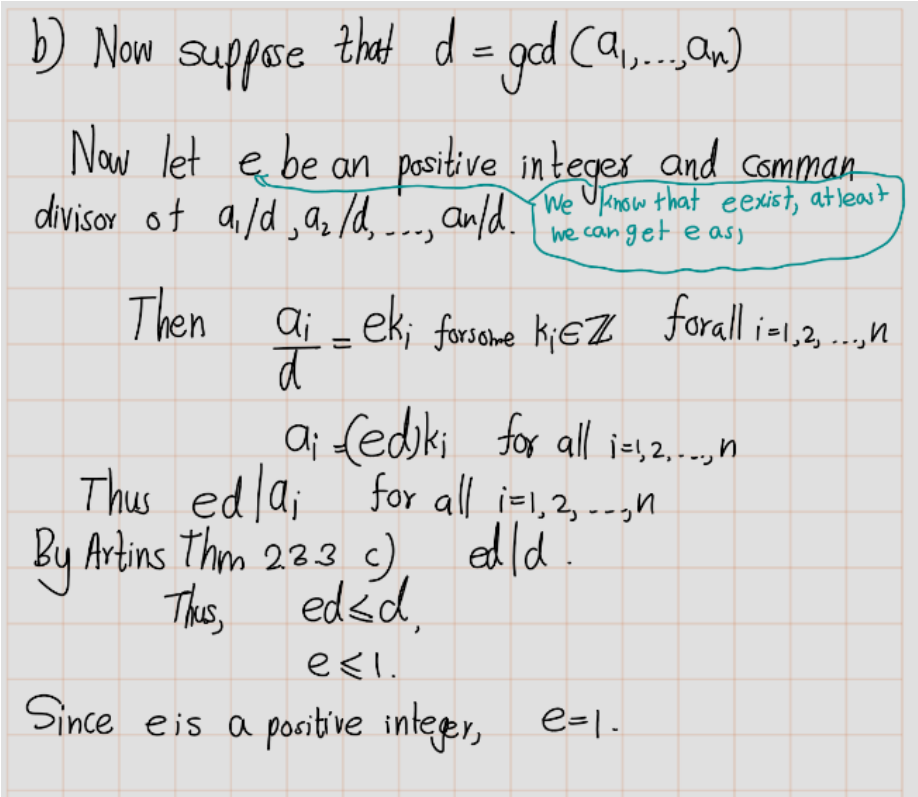
Solution:

a.




Therefore S is a subgroup of Z.
By artins book thm 2.3.3 there exist a positive integer d such that
dZ = a1Z + --- + anZ
This d is define as gcd(a1,...,an)
Linear Combination
Note that d ∈ Zd = S = a1Z + --- + anZ
Thus, there exist r1,...,rn ∈ Z such that
d = r1a1 + --- + rnan

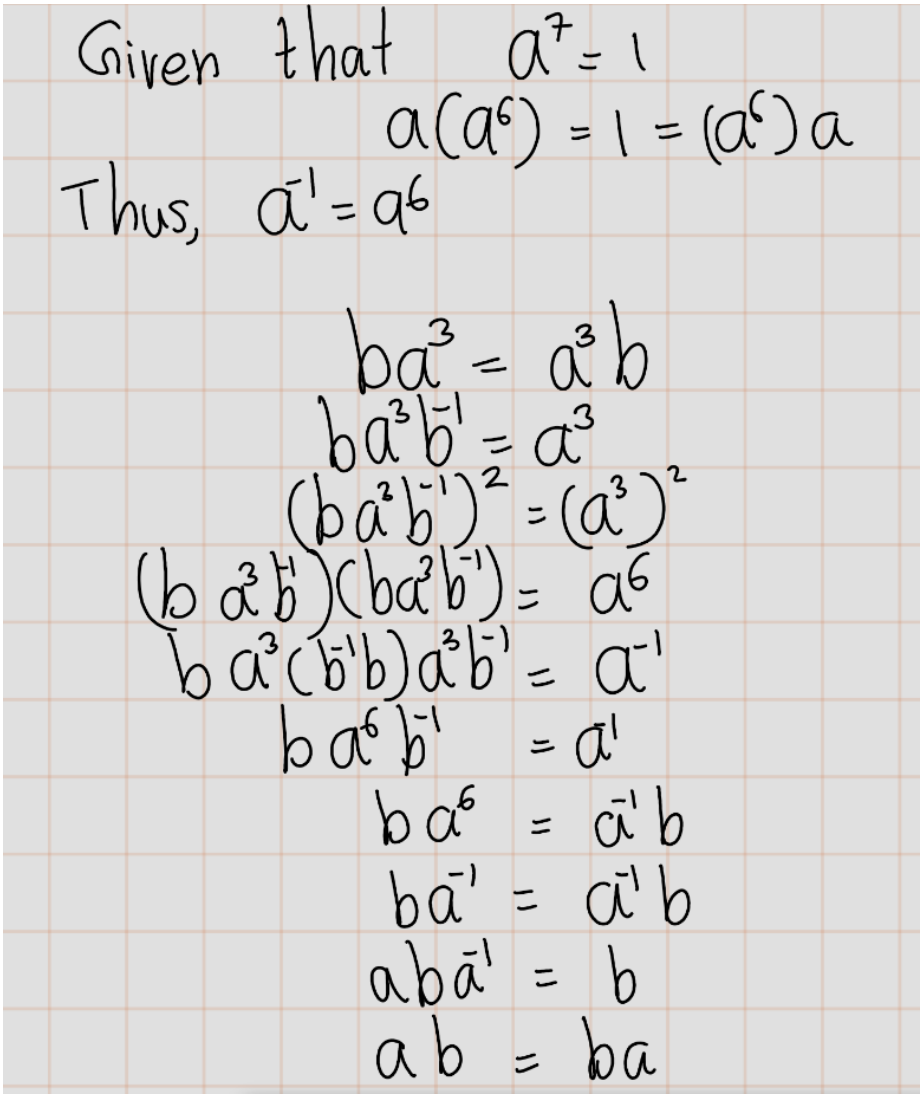
b.



Cyclic group

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

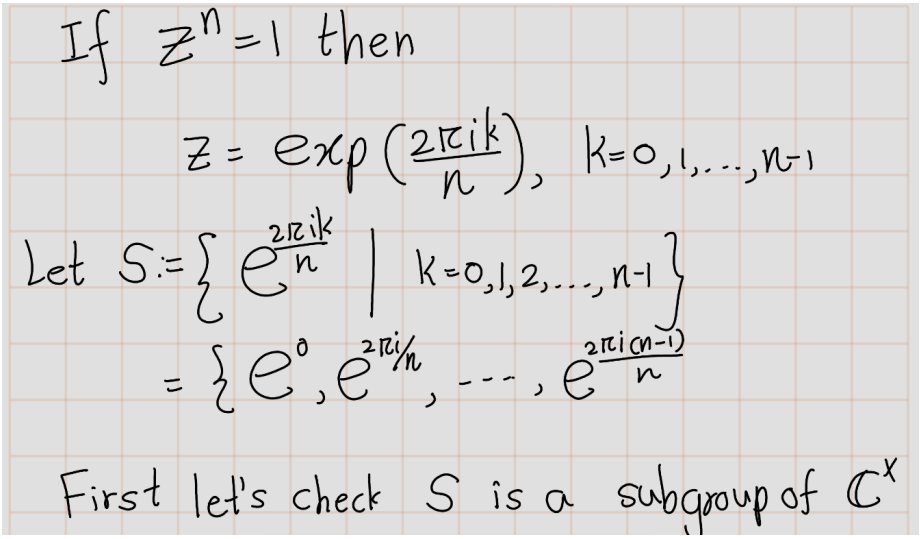
Solution:

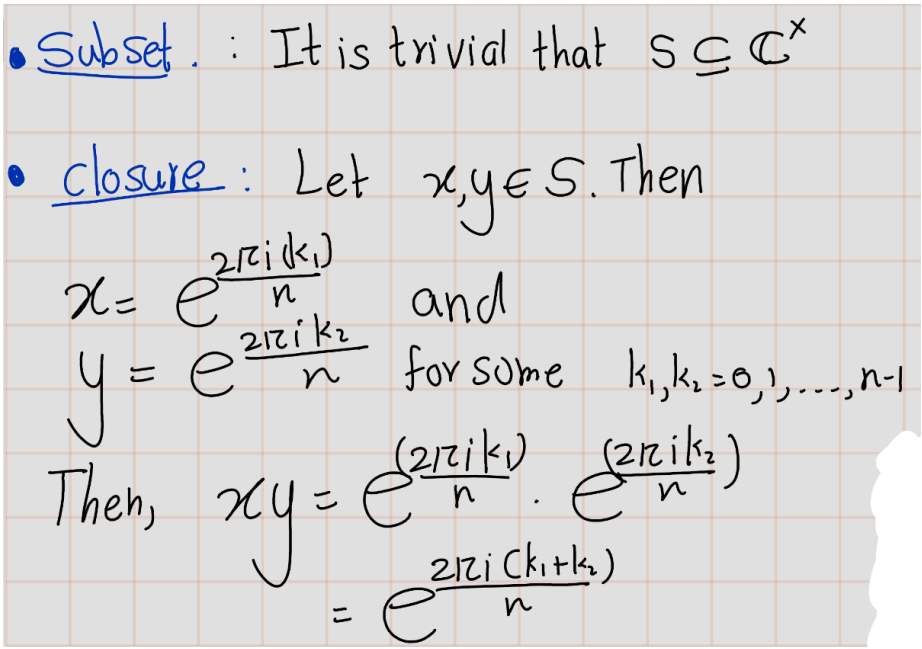


An nth root of unity is a complex number z such that $z^n = 1$.

(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.

Solution:


If $z^n = 1$ then
$z = \exp\left(\frac{2\pi i k}{n}\right)$, $k = 0, 1, \ldots, n-1$
Let $S := \left\{ e^{\frac{2\pi i k}{n}} \mid k = 0, 1, 2, \ldots, n-1 \right\}$
$= \left\{ e^0, e^{2\pi i/n}, \ldots, e^{\frac{2\pi i(n-1)}{n}} \right\}$
First let's check S is a subgroup of $\mathbb{C}^\times$


• Subset. : It is trivial that $S \subseteq \mathbb{C}^\times$
• closure : Let $x, y \in S$. Then
$x = e^{\frac{2\pi i(k_1)}{n}}$ and
$y = e^{\frac{2\pi i k_2}{n}}$ for some $k_1, k_2 = 0, 1, \ldots, n-1$
Then, $xy = e^{\frac{(2\pi i k_1)}{n}} \cdot e^{\frac{(2\pi i k_2)}{n}}$
$= e^{\frac{2\pi i(k_1+k_2)}{n}}$

If $(k_1+k_2) > n$, we can find $a, b \in \mathbb{N}$ such that (by divison algrothm)

$$k_1 + k_2 = an + b, \quad 0 \le b < n$$

$$\begin{aligned} xy &= e^{\frac{2\pi i (k_1+k_2)}{n}} \\ &= e^{\frac{2\pi i}{n}(an+b)} \\ &= \underbrace{e^{2\pi i (a)}} \cdot e^{\frac{2\pi i b}{n}} \\ &= 1 \times e^{\frac{2\pi i b}{n}} \\ &= e^{2\pi i b/n} \quad \text{, for some } b = 0, 1, 2, \ldots, n-1 \end{aligned}$$

Thus, $xy \in S$

- Inverse: Let $x \in S$.
  - If $x = 1$, then $x^{-1} = 1$.
  - If $x \neq 1$,

Then $x = \exp(2\pi i k_1/n)$ for some $k_1 = 1, 2, \ldots, n-1$

Choose $y = \exp(2\pi i(n-k_1)/n)$

Then,

$$yx = xy = e^{\frac{2\pi i k_1}{n}} \cdot e^{\frac{2\pi i(n-k_1)}{n}} = e^{\frac{2\pi i(k_1+n-k_1)}{n}}$$
$$= e^{(2\pi i n)/n} = e^{2\pi i} = 1$$

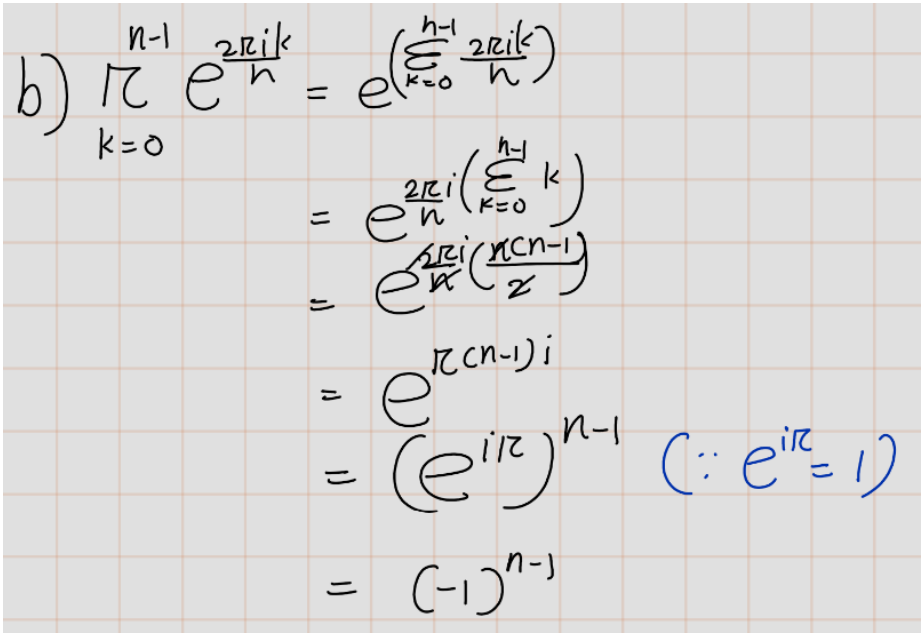
Thus, $x^{-1} = y \in S$.

By subgroup test S is a subgroup of G

Now, we are done subgrouping. Now we have to look the cyclic property.

Observe that $\left(e^{\frac{2\pi i}{n}}\right)^k = e^{\frac{2\pi k i}{n}}$, $k = 0, 1, \ldots, n-1$

Therefore, $S = \langle e^{\frac{2\pi i}{n}} \rangle$



Let a and b be elements of a group G. Prove that ab and ba have the same order

Let a and b be elements in a group G with identity e.

Suppose that ab has finite order n. Then $(ab)^n = e$ and n is the smallest positive integer for which this equation is true. We also have that

$$(ba)^{n+1} = (ba)(ba)\cdots(ba) = b\underbrace{(ab)\cdots(ab)}_{n \text{ times}}a = b(ab)^n a = a(ba)^m b = bea = ba.$$

Thus, since $(ba)^{n+1} = (ba)^n(ba)$ we can conclude that $(ba)^n(ba) = ba$ and then by the cancellation law, we have that $(ba)^n = e$.

Now, to show that the order of ba is n, we need to demonstrate that n is the smallest positive integer such that $(ba\hat{}\mathrm{n} = \mathrm{e}.\ )$

Suppose there exists a positive integer $m < n$ such that $(ba)^m = e$. Then,

$$(ab)^{m+1} = (ab)(ab)\cdots(ab) = a\underbrace{(ba)\cdots(ba)}_{m \text{ times}}b = a(ba)^m b = aeb = ab.$$

Thus, since$(ab)^{m+1} = (ab)^m(ab)$ we have that $(ab)^m(ab) = ab$ and then by the cancellation law, we have that $(ab)^m = e$ which contradicts the fact that n is the smallest positive integer such that $(ab)^n = e$.

Hence, n is the smallest positive integer such that $(ba)^n = e$ and therefore (ba) has finite order n.

Describe all groups G that contain no proper subgroup

Solution:

The easyist example is the trivial group. $\{1\}$
But we are not intertested.
Let G be a non-trivial group no proper subgroup.

Claim: G is cyclic.
Assume that G is not cyclic.
Since $G \neq \{1\}$, there exist $1 \neq a, b \in G$, such that

$$b \notin \langle a \rangle$$

Thus $\langle a \rangle$ is proper subgroup of G.
Since $a \neq 1$, $\langle a \rangle \neq \{1\}$. This is
contradict the choice of G.
Therefore G is cyclic.
Therefore there exist $p \in G$ such that
$G = \langle p \rangle$ here $p \neq 1$.

claim: G has a finite order.

Assume the contray, G has infinite order.
Then consider, $H = \langle p^2 \rangle$
Note that $H \leq G$. Since $p \notin \langle p^2 \rangle = H$, H is proper subgroup. This contradict the choice of G. There H has finite order.

So, let's say G has order n. (i.e: $|G| = |\langle p \rangle| = n$)

$$G = \langle p \rangle := \{1, p, p^2, \cdots, p^{n-1}\}$$

So, let's investigate further,
Let's consider $H' := \langle p^k \rangle$, where $k = 0, 1, \ldots, n-1$

- if $k=0$ then $H' = \langle 1 \rangle = \{1\}$ trivial group that we are interest
- if $k=1$ then $H' = \langle p \rangle = H$, this gives whole group.
- otherwise
  Let $d = \gcd(k, n)$. By Artins Thm 2.4.3, order of p^k is n/d. Thus, $|\langle p^k \rangle| = n/d$.

if $d \neq 1$, then there might be a problem
if $d \neq 1$, then $\langle p^k \rangle$ is proper subgroup. Because of the number of elements.

claim: Order of G is prime.

Assume the contray that order of $G = n$ is not prime
Previosly, we saw that $\langle p^k \rangle = H'$ is proper subgroup
So, it is contradiction. Thus G has prime order.

Therefore it is nessary for G to be prime order.
Is it sufficient ?

Let G be a cyclic goroup of prime order.
Let $G = \langle p \rangle$ and $|G| = |\langle p \rangle| = n$; n is a prime number.
Then "Has G have prime order?"
Let H be a non-trivial subgroup of G.
Define,
$S = \{ k \mid k \in \{1, 2, \ldots, n\} \text{ and } p^k \in H \} \subseteq \{1, 2, \ldots, n\}$
Let $k_0 = \min(S)$. By well-ordering principle we know that min(S) exists.

claim: $H = \langle p^{k_0} \rangle$

subclaim1: $\langle p^{k_0} \rangle \subseteq H$.

Note that $p^{k_0} \in H$.

Let $x \in \langle p^{k_0} \rangle$. Then $x = (p^{k_0})^m$ forsome $m \in \mathbb{Z}$

Thus $x = \underbrace{p^{k_0} \cdot p^{k_0} \cdots p^{k_0}}_{m\text{-times}} \in H$ (Since H is a group.)

$\langle p^{k_0} \rangle \subseteq H$

subclaim2: $\langle p^{k_0} \rangle \supseteq H$.

Let $y \in H$. Since H is an subgroup of G. $y \in G$.

Then, $y = p^l$ forsome l.

By division algrothmn, $l = q k_0 + r$, where $0 \leq r < k_0$

$$y = p^l = p^{(qk_0 + r)} = (p^{k_0})^q \cdot p^r$$

claim: $a^r \in H$.

Note that $p^l \in H$ and $(p^{k_0})^q \in H$. Thus,

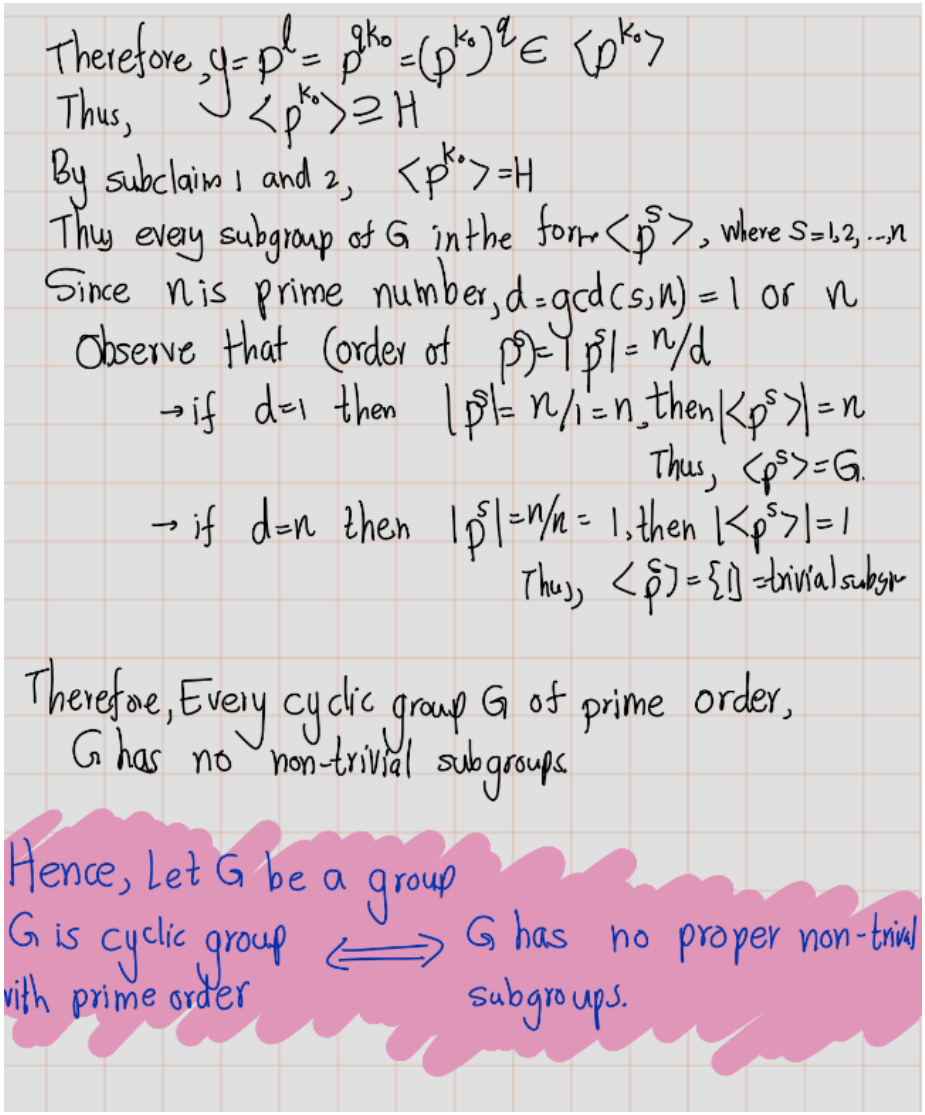
$$p^r = p^{l - k_0 q} = p^l \cdot \left((p^{k_0})^q\right)^{-1} \in H.$$

claim: $r = 0$

Otherwise, if $r > 0$, Since $p^r \in H$, then $r \in S$.

Since $r < k_0$. This is a contradict the k_0 is the min(S).

Thus $r = 0$.



Prove that every subgroup of a cyclic group is cyclic. Do this by working with exponents, and use the description of the subgroups of $(\mathbb{Z}, +)$.

Let G be a cylic group. Let $G = \langle a \rangle$
Let H be an subgroup of G $(H \leq G)$.
Define

$$S := \{ k \in \mathbb{Z} \,,\, a^k \in H \}$$

Claim: $S \leq (\mathbb{Z}, +)$

- subset ?: It is trival $S \subseteq (\mathbb{Z}, +)$
- closure?: Let $k_1, k_2 \in S$, Then $a^{k_1}, a^{k_2} \in H$. So,
  $a^{(k_1+k_2)} = a^{k_1} \cdot a^{k_2} \in H$ (Since H is subgroup)
  Thus, $k_1 + k_2 \in S$.
- Inverse?: Let $k_1 \in S$. So, $a^{k_1} \in H$. Then $a^{-k_1} = (a^{k_1})^{-1} \in H$
  (Because H is subgroup)
  $a^{-k_1} \cdot a^{k_1} = a^{-k_1+k_1} = a^0 = 1 = a^0 = a^{k_1-k_1} = a^{k_1} \cdot a^{-k_1}$
  Thus, $-k_1 + k_1 = 0 = k_1 - k$, Thus, inverse of k_1 is $-k_1$

There fore $(S, +)$ is an subgroup of $(\mathbb{Z}, +)$.
i.e: $(S, +) \leq (\mathbb{Z}, +)$

- If $S = \{0\}$, then $H = \{1\}$ = trivial subgroup.
- If S is not trivial, by Artins Algebra book 2.33
  $\exists\, b \in \mathbb{Z}$ such that $S = b\mathbb{Z}$.

So,

$$H := \{ a^k \mid k \in S \} = \{ a^k \mid k \in b\mathbb{Z} \}$$
$$= \{ a^{ib} \mid i \in \mathbb{Z} \} = \langle a^b \rangle$$

(a) Let G be a cyclic group of order 6. How many of its elements generate G? Answer the same question for cyclic groups of orders 5 and 8.
(b) Describe the number of elements that generate a cyclic group of arbitrary order n.

Solution:

a)

CASE I: Order = 6

Let G be a cyclic group with order 6.

Let's say $G = \langle a \rangle$,

$$G := \{a^0 = 1, a^1, a^2, a^3, a^4, a^5\}$$

By Artin's book proposition 2.4.3,

$$|a^k| = |\langle a^k \rangle| = \frac{6}{\gcd(6,k)}, \text{ for all } k \in \{1, \dots, 5\}$$

$$\langle a^k \rangle = \langle a \rangle \iff |\langle a^k \rangle| = |\langle a \rangle|$$
$$\iff \frac{6}{\gcd(6,k)} = 6$$
$$\iff \gcd(6,k) = 1$$
$$\iff k = 1 \text{ or } k = 5$$

$\langle a^1 \rangle = \langle a^5 \rangle = G$

So, a, a^5 generate G.

CASE 2: order = 5

Let G be a cyclic group with order 5.

Let's say $G = \langle a \rangle$,

$G := \{a^0 = 1, a^1, a^2, a^3, a^4\}$

By Artin's book proposition 2.4.3,

$$|a^k| = |\langle a^k \rangle| = \frac{5}{\gcd(5,k)}, \text{ for all } k \in \{1, \ldots, 5\}$$

$$\langle a^k \rangle = \langle a \rangle \iff |\langle a^k \rangle| = |\langle a \rangle|$$

$$\iff \frac{5}{\gcd(6,k)} = 5$$

$$\iff \gcd(5,k) = 1$$

$$\iff k = 1, 2, 3, 4$$

$$\langle a^1 \rangle = \langle a^2 \rangle = \langle a^3 \rangle = \langle a^4 \rangle = G.$$

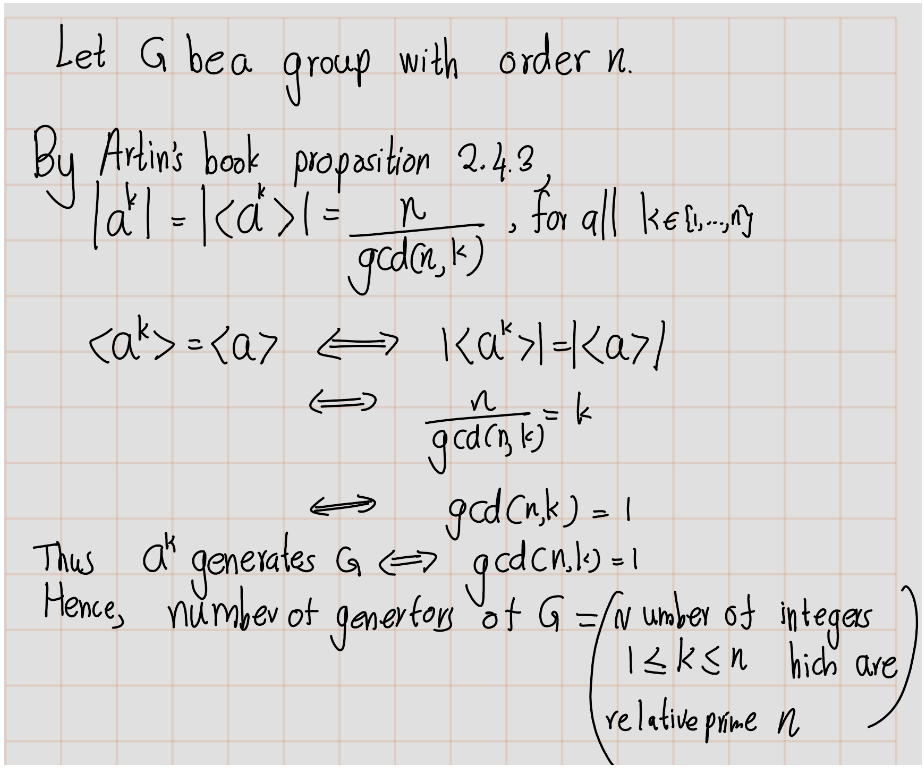
a^1, a^2, a^3, a^4 generate G.

CASE-III Order = 8

Similar to above case, we can obtain that

a^1, a^3, a^5, a^7 generates G.

b)



Let x and y be elements of a group G. Assume that each of the elements x, y, and xy has order 2. Prove that the set $H = \{I, x, y, xy\}$ is a subgroup of G, and that it has order 4.

Let G be a group and $x, y \in G$. Suppose that
$|x| = |y| = |xy| = 2$
Let $H = \{1, x, y, xy\}$.

claim: $H \leq G$.

- subset: $H \subseteq G$. (It is trivial that $1, x, y \in G$ and since $x, y \in G$, $xy \in G$)
- closure:

$\cdot$	1	x	y	xy
1	1	x	y	xy
x	x	1	xy	y
y	y	$yx=xy$	1	$yxy = y^2x = x$
xy	xy	$xyx = x^2y = y$	x	1

By multiplication table, we can gurentee the closure

claim: $xy = yx$

First of we have observe that
$x^2 = y^2 = (xy)^2 = 1$
Thus inverse of those elements are itself.
i.e: $x^{-1} = x$, $y^{-1} = y$, $(xy)^{-1} = xy$ — (*)

$(xy)^2 = (xy)(xy) = 1$

$(xyxy)y^{-1} = y^{-1}$

$xyx = y^{-1}$

$xyxx^{-1} = y^{-1}x^{-1}$

$xy = y^{-1}x^{-1} = yx$ (by ⊛)

- Inverse: $x^{-1} = x$, $y^{-1} = y$, $(xy)^{-1} = xy \in H$.

Therefore, H is a subgroup of G.

claim: $|H| = 4$

- Since x, y, xy has order 2, H is not trivial. In other words, $|H| \neq 1$.

+ claim: $x \neq y$

if $x = y$, then $xy = x^2 = 1$. This contrdict the $|xy| = 2$.

+ claim: $x \neq xy$

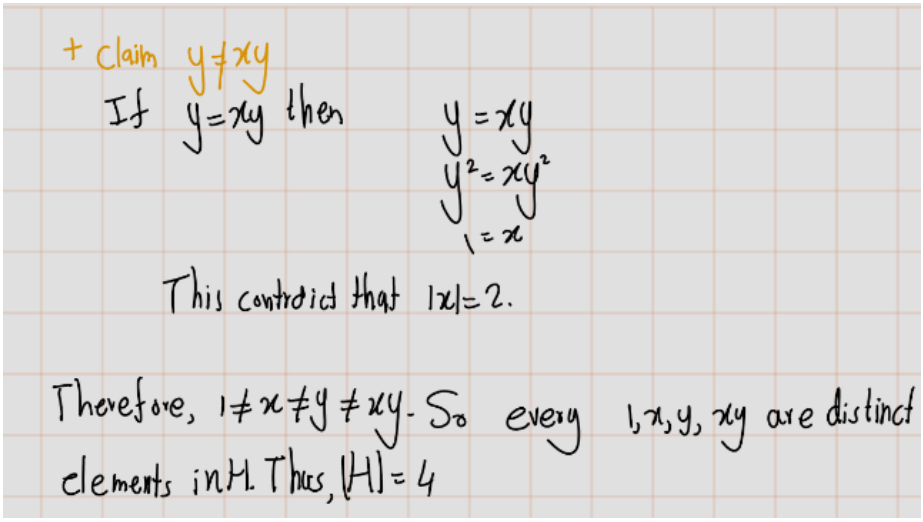
if $x = xy$ then, $x = xy$

$xx = xxy$

$x^2 = x^2y$

$1 = y$.

This contrdict that $|y| = 2$.



a) Prove that the elementary matrices of the first and third types (1.2.4) generate $GL_n(\mathbb{R})$.
b) Prove that the elementary matrices of the first type generate $SL_n(K)$. Do the 2×2 case first.

Recall the types of elementary matrices,

(1.2.4)

Type (i):

$$\begin{array}{c} \\ i \\ \\ j \\ \\ \end{array}\!\!\begin{array}{c} \begin{array}{cccccc} i & & & j & & \end{array} \\ \begin{bmatrix} 1 & & & & & \\ & 1 & & a & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{bmatrix} \end{array} \quad \text{or} \quad \begin{array}{c} \\ j \\ \\ i \\ \\ \end{array}\!\!\begin{array}{c} \begin{array}{cccccc} j & & & i & & \end{array} \\ \begin{bmatrix} 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & a & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{bmatrix} \end{array} \quad (i \neq j).$$

One nonzero off-diagonal entry is added to the identity matrix.

Type (ii):

$$\begin{array}{c} \\ i \\ \\ j \\ \\ \end{array}\!\!\begin{array}{c} \begin{array}{cccccc} i & & & j & & \end{array} \\ \begin{bmatrix} 1 & & & & & \\ & 0 & & 1 & & \\ & & 1 & & & \\ & 1 & & 0 & & \\ & & & & 1 & \\ & & & & & 1 \end{bmatrix} \end{array}$$

The ith and jth diagonal entries of the identity matrix are replaced by zero, and 1's are added in the (i, j) and (j, i) positions.

Type (iii):

$$\begin{array}{c} \\ i \\ \\ \\ \\ \end{array}\!\!\begin{array}{c} \begin{array}{cccccc} & & i & & & \end{array} \\ \begin{bmatrix} 1 & & & & & \\ & 1 & & & & \\ & & c & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{bmatrix} \end{array} \quad (c \neq 0).$$

One diagonal entry of the identity matrix is replaced by a nonzero scalar c.

Homomorphisms

Isomorphisms

Equivalence Relations and Partitions

Cosets

Modular Arthmetic

What are the possible values of a^2 modulo 4? modulo 8?

solution:

- *In modulo 4*

$$\begin{aligned}\overline{0}^2 &\equiv 0 \pmod 4\\ \overline{1}^2 &\equiv 1 \pmod 4\\ \overline{2}^2 &\equiv 0 \pmod 4\\ \overline{3}^2 &\equiv 1 \pmod 4\end{aligned}$$

The possible values of $a^2 \pmod 4$ are 0 and 1.

- *In modulo 8*

$$\begin{aligned}\overline{0}^2 &\equiv 0 \pmod 8\\ \overline{1}^2 &\equiv 1 \pmod 8\\ \overline{2}^2 &\equiv 4 \pmod 8\\ \overline{3}^2 &\equiv 1 \pmod 8\\ \overline{4}^2 &\equiv 0 \pmod 8\\ \overline{5}^2 &\equiv 1 \pmod 8\\ \overline{6}^2 &\equiv 4 \pmod 8\\ \overline{7}^2 &\equiv 1 \pmod 8\end{aligned}$$

The possible values of $a^2 \pmod 8$ are 0,1 and 4.

Prove that every integer a is congruent to the sum of its decimal digits modulo 9.

Let $x \in \mathbb{Z}$. Now we can represent x as follows

$$x = a_0 10^0 + a_1 10^1 + \cdots + a_n 10^n = \sum_{i=0}^{n} a_i 10^i \text{ forsome } n \in \mathbb{Z}, \text{ and } a_i \in \{0, 1, ..., 9\}$$

We need to show $x \equiv \sum_{i=0}^{n} a_i \pmod 9$. So, now consider,

$$\begin{aligned} x - \sum_{i=0}^{n} a_i &= \sum_{i=0}^{n} a_i 10^i - \sum_{i=0}^{n} a_i && (69)\\ &= \sum_{i=0}^{n} (a_i 10^i - a_i) && (70)\\ &= \sum_{i=0}^{n} a_i (10^i - 1) && (71)\end{aligned}$$

By follwing calim we can get that,

$$x - \sum_{i=0}^{n} a_i \equiv 0 \pmod 9 \tag{72}$$

$$x \equiv \sum_{i=0}^{n} a_i \pmod 9 \tag{73}$$

Claim: $9|(10^k - 1)$ for any $k \in \mathbb{N}$.

We use mathematical induction.
$k = 1$
This case is trivial. Because $9|10 - 1$.
$k = n \in \mathbb{Z}$
Now asuume when $n = k, 9|(10^n - 1)$.
$k = n + 1$

$$10^{n+1} - 1 = 10 \cdot 10^n - 1 = 9 \cdot 10^n + (10^n - 1)$$

Thus $9|(10^{n+1} - 1)$.
Therefore,by mathematical induction, $9|(10^n - 1)$ for any $n \in \mathbb{N}$.

Solve the congruence $2x \equiv 5$ modulo 9 and modulo 6.

Done Later add.

Determine the integers n for which the pair of congruences $2x - y \equiv 1$ and $4x + 3y \equiv 2$ modulo n has a solution.

Done Later add.

Prove the Chinese Remainder Theorem: Let a, b, u, v be integers, and assume that the greatest common divisor of a and b is 1. Then there is an integer x such that $x \equiv u$ modulo a and $X \equiv v$ modulo b.
Hint: Do the case $u = 0$ and $v = 1$ first.

Determine the order of each of the matrices A and B when the matrix entries are interpreted modulo 3.

Product Group

Let x be an element of order r of a group G, and let y be an element of G' of order s. What is the order of (x, y) in the product group $G \times G'$?

Solution: The order of (x, y) in the product group $G \times G'$ is $lcm(r, s)$
Let $n \in \mathbb{Z}^+$ such that

$$(x, y)^n = (x^n, y^n) = (1_G, 1_{G'}).$$

This implies, $x^n = 1_G$ and $y^n = 1_{G'}$. Since order of x and y are r and s respectively,

$$r|n \quad \text{and} \quad s|n$$

So, we know that the least positive integer such that above property holds is $lcm(r, s)$. Hence,The order of (x, y) in the product group $G \times G'$ is $lcm(r, s)$.

What does Proposition @ref(prp:prp2114) tell us when, with the usual notation for the symmetric group S_3, K and H are the subgroups $< y >$ and $< x >$?

Recall: $y^2 = 1$ and $x^3 = 1$. Then

$$H =< x >= \{1, x, x^2\} \quad \text{and} \quad K =< y >= \{1, y\}$$

Let the multiplication map, $f : H \times K \to S_3$ defined by $f(h, k) = hk$. Then, $Im(f) = HK = \{hk : h \in < x >, k \in < y >\} = \{1, x, x^2, y, xy, x^2y\}$.

Claim 1: f is injective.
Observe that $H \cap K = \{1\}$. by @ref(prp:prp2114) a) f is injective.

Claim 2: f is surjective.
Observe that $S_3 = HK = \{1, x, x^2, y, xy, x^2y\}$. Thus, f is surjective.

Claim 3 : f is not homomorphism.

$$f((x, y) \cdot (x, 1)) = f(x^2, y^2) = f(x^2, 1) = x^2 \cdot 1 = x^2 \tag{74}$$
$$f(x, y) \cdot f(x, 1) = (x \cdot y) \cdot (x \cdot 1) = (xy) \cdot x = y \tag{75}$$

Thus, f is not a homomorphism.

Prove that the product of two infinite cyclic groups is not infinite cyclic.

- **Claim 1** : Infinite cyclic groups are isomorphic to Z.
  Let G be a infinte cyclic group and $< a >= G$. We can define a function $f : \mathbb{Z} \to G$ by $f(n) = a^n$ for all integers n. We need to show that f is an isomorphism, which means it is bijective.
  - **Subclaim 1.1** : f is a hormorphism.

    $$f(n + m) = a^{n+m} = a^n \cdot a^m = f(n) \cdot f(m)$$

    Thus, f is a hormorphism.
  - **Subclaim 1.2** :f is a injective
    Suppose that $f(n) = f(m)$

    $$f(n) = f(m) \tag{76}$$
    $$a^n = a^m \tag{77}$$
    $$n = m \ \text{(Since order is infinite)} \tag{78}$$

– **Subclaim 1.3** : f is surjective.
Let $x \in G =< a >$. Then, $x = a^k$ for some $k \in \mathbb{Z}$. Then, observe that

$$f(k) = a^k = a$$

. Thus, f is surjective.

Therefore, f is an isomorphism. Thus, the infinite cyclic groups are isomorphic to $\mathbb{Z}$.

We can consider $\mathbb{Z} \times \mathbb{Z}$. Suppose that (a, b) generate the product group. But then, we see that $(2a, b)$ cannot be obtained from adding (a, b) to itself, which implies that $\mathbb{Z} \times \mathbb{Z}$ is not infinite cyclic.

In each of the following cases, determine whether or not G is isomorphic to the product group $H \times K$.

(a) $G = \mathbb{R}^\times$, $H = \{\pm 1\}$, $K = \{\text{positive real numbers}\}$.

(b) $G = \{\text{invertible upper triangular } 2\times 2 \text{ matrices}\}$, $H = \{\text{invertible diagonal matrices}\}$, $K = \{\text{upper triangular matrices with diagonal entries } 1\}$.

(c) $G = e^x$, $H = \{\text{unit circle}\}$, $K = \{\text{positive real numbers}\}$.

Solution:

(a) Observe that $G = \mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ is abelian. Then $H, K \trianglelefteq G$. Further, observe that $H \cap K = \{1\}$ and $HK = \mathbb{R}^\times = G$. Thus, by proposition @ref(prp:prp2114) $G \cong H \times K$.

(b)

- **Claim b.1**: $K \trianglelefteq G$.
Let $g = \begin{bmatrix} a & b \\ & c \end{bmatrix}$ be an arbitary matrix in G and $k = \begin{bmatrix} 1 & d \\ & 1 \end{bmatrix} \in K$. Then,

$$g^{-1} = \begin{bmatrix} a^{-1} & -ba^{-1}c^{-1} \\ & c^{-1} \end{bmatrix}$$

Then

$$gkg^{-1} = \begin{bmatrix} a & b \\ & c \end{bmatrix} \begin{bmatrix} 1 & d \\ & 1 \end{bmatrix} \begin{bmatrix} a^{-1} & -ba^{-1}c^{-1} \\ & c^{-1} \end{bmatrix}$$

$$= \begin{bmatrix} a & b \\ & c \end{bmatrix} \begin{bmatrix} a^{-1} & dc^{-1} - ba^{-1}c^{-1} \\ & c^{-1} \end{bmatrix} = \begin{bmatrix} 1 & adc^{-1} \\ & 1 \end{bmatrix} \in K$$

Thus, $H \trianglelefteq G$.

- **Claim b.2** : $H = Z(G)$ (H is in the center of G).

– *subclaim b.2.1* : $H \subseteq Z(G)$.
Let $h = \begin{bmatrix} x & 0 \\ & x \end{bmatrix} \in H$. Then,

$$B = \begin{bmatrix} x & 0 \\ & x \end{bmatrix} = x \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} = BI$$

Then observe that, for any $A \in G$,

$$BA = (xI)A = xA = Ax = A(xI) = AB$$

– *subclaim b.2.2* : $H \supseteq Z(G)$.
Let $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \in Z(G)$, then,

$$\begin{bmatrix} p & q \\ r & s \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} p & q \\ r & s \end{bmatrix} \tag{79}$$

$$\begin{bmatrix} p & -q \\ r & -s \end{bmatrix} = \begin{bmatrix} p & q \\ -r & -s \end{bmatrix} \tag{80}$$

$$\tag{81}$$

This yields $-q = q$ and $r = -r$ which imply $q = r = 0$. Now considering,

$$\begin{bmatrix} p & 0 \\ 0 & s \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} p & 0 \\ 0 & s \end{bmatrix} \tag{82}$$

$$\begin{bmatrix} 0 & p \\ q & 0 \end{bmatrix} = \begin{bmatrix} 0 & q \\ p & 0 \end{bmatrix} \tag{83}$$

$$\tag{84}$$

This implies that $a = d$ and since the matrix is invertible, $a \neq 0$. Thus, $H \supseteq Z(G)$.

Therefore, $H = Z(G)$. In other words, H is in the center of G.

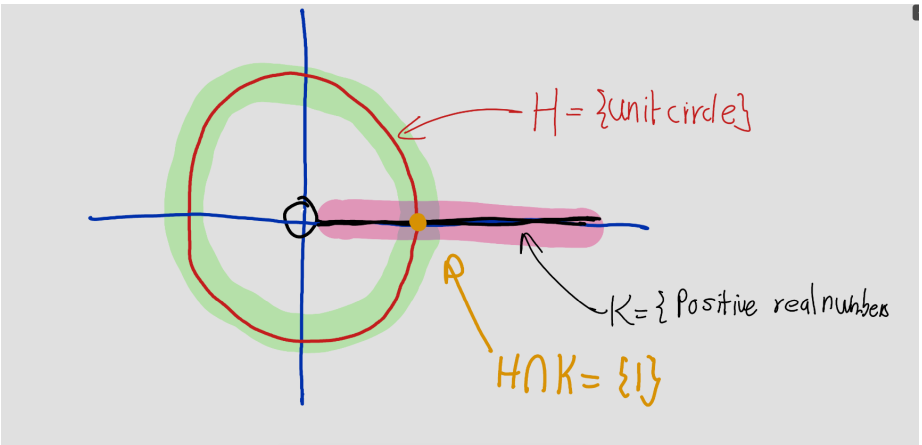
- **Claim b.2** : $H \trianglelefteq G$.
Since, H is in the center of G, then H is normal.
- **Claim b.3** : $H \cap K = \{I\}$.
This is trivial.
- **Claim b.4** : $HK = G$ Clearly, $HK \subseteq G$. Conversely, for any $g \in G$, $a \neq 0, b \neq 0$,

$$g = \begin{bmatrix} a & b \\ & c \end{bmatrix} = \begin{bmatrix} a & \\ & c \end{bmatrix} \begin{bmatrix} 1 & a^{-1}b \\ & 1 \end{bmatrix} \in HK$$

. Thus, $HK = G$.

Therefore, by proposition @ref(prp:prp2114) $G \cong HK$

(c) Since $C^\times$ is abelian, then H and K are normal. And, $H \cap K = \{1\}$.

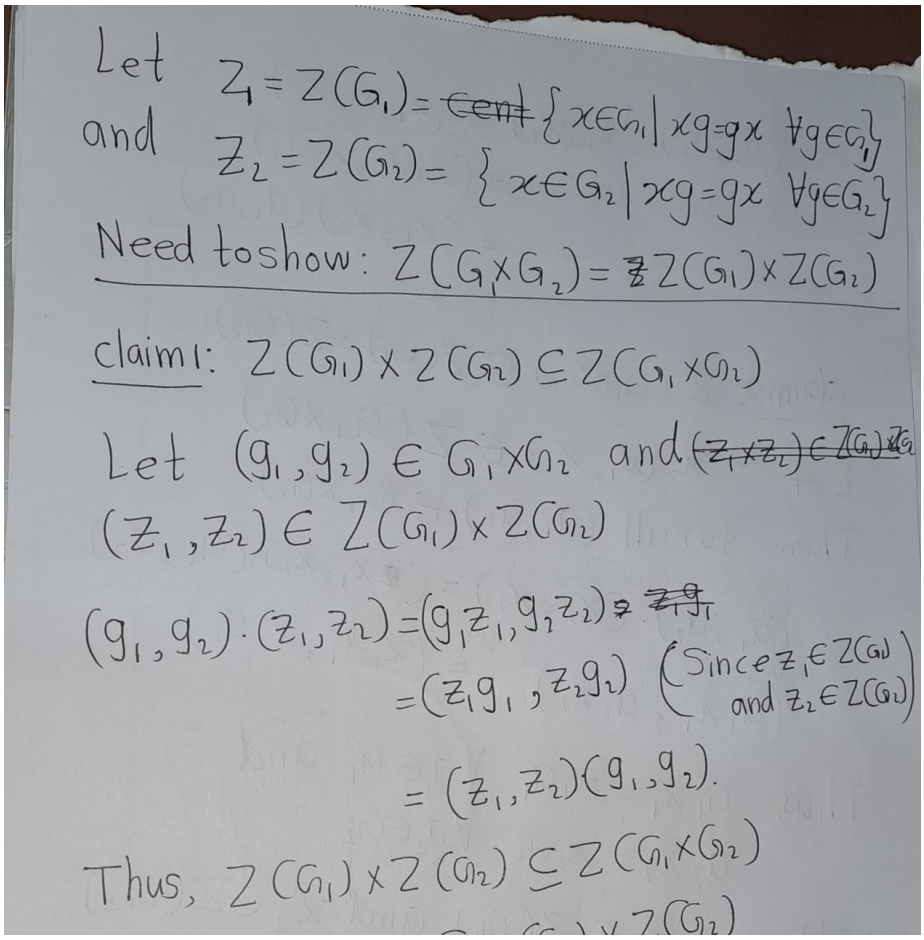


Consider $a + bi \in C^\times$. Then

$$a + bi = \left(\frac{a}{\sqrt{a^2 + b^2}} + \frac{b}{\sqrt{a^2 + b^2}} i \right) \sqrt{a^2 + b^2} \in HK$$

So, $HK = G$. So, by proposition @ref(prp:prp2114) $G \cong H \times K$.

Let G_1 and G_2 be groups, and let Z_i be the center of G_i. Prove that the center of the product group $G_1 \times G_2$ is $Z_1 \times Z_2$.



Let $Z_1 = Z(G_1) = \{x \in G_1 \mid xg = gx \ \forall g \in G_1\}$
and $Z_2 = Z(G_2) = \{x \in G_2 \mid xg = gx \ \forall g \in G_2\}$

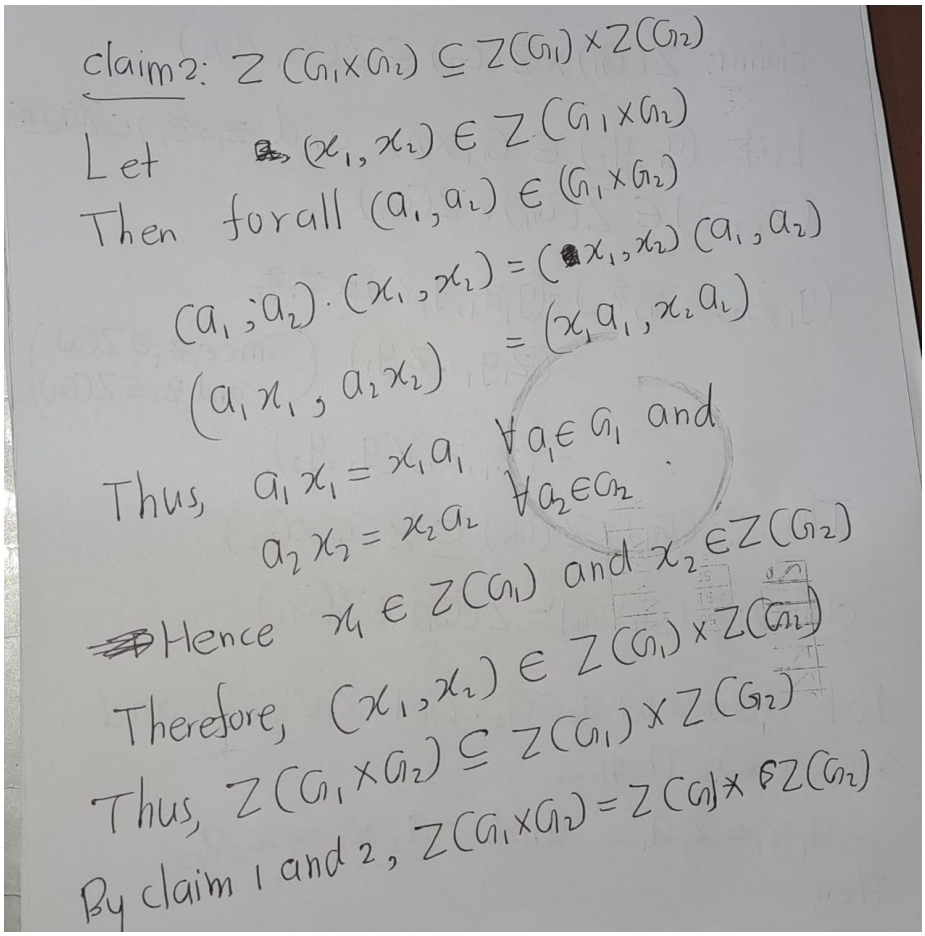
Need to show: $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$

claim1: $Z(G_1) \times Z(G_2) \subseteq Z(G_1 \times G_2)$

Let $(g_1, g_2) \in G_1 \times G_2$ and $(z_1, z_2) \in Z(G_1) \times Z(G_2)$

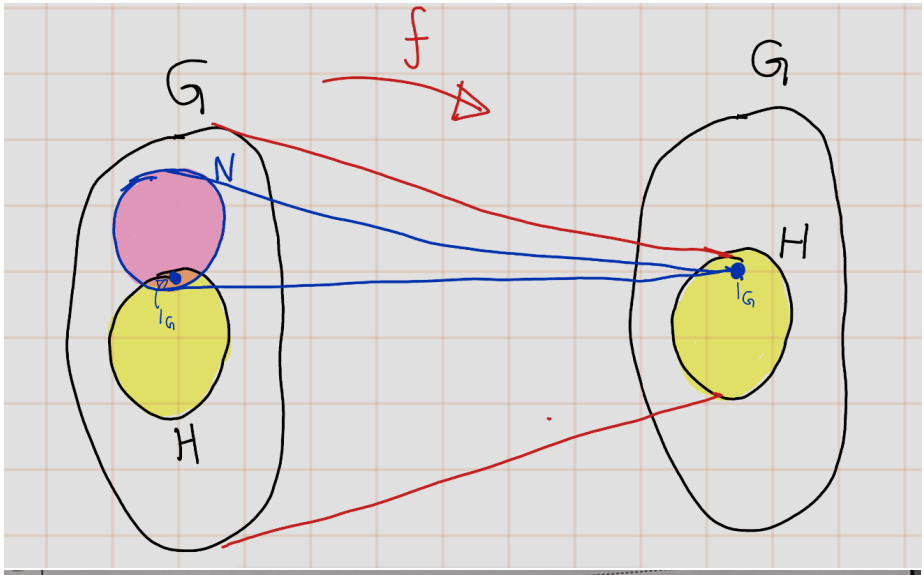
$(g_1, g_2) \cdot (z_1, z_2) = (g_1 z_1, g_2 z_2)$
$= (z_1 g_1, z_2 g_2)$ (Since $z_1 \in Z(G_1)$ and $z_2 \in Z(G_2)$)
$= (z_1, z_2)(g_1, g_2)$.

Thus, $Z(G_1) \times Z(G_2) \subseteq Z(G_1 \times G_2)$



Let G be a group that contains normal subgroups of orders 3 and 5, respectively. Prove that G contains an element of order 15.

Let H be a subgroup of a group G, let $\phi : G \to H$ be a homomorphism whose restriction to H is the identity map, and let N be its kernel. What can one say about the product map $H \times N \to G$?



Claim: f is injective.

Clearly $1_G \in H \cap N$

Assume that $1_G \neq x \in H \cap N$

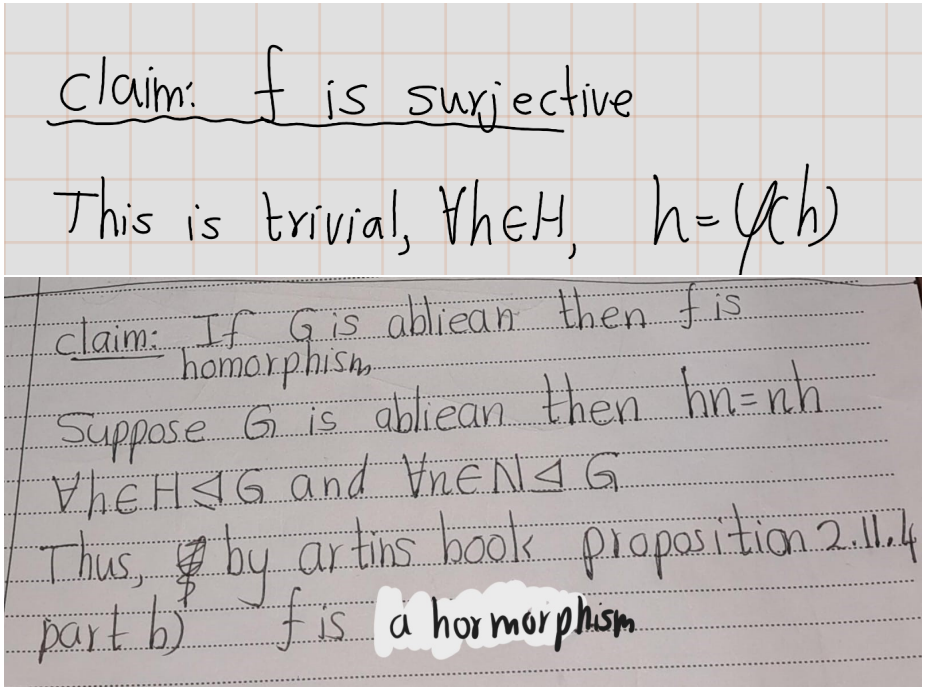
$x \in H \Rightarrow \varphi(x) = x \neq 1_G$ — (1)

$x \in N \Rightarrow \varphi(x) = 1_G$ — (2)

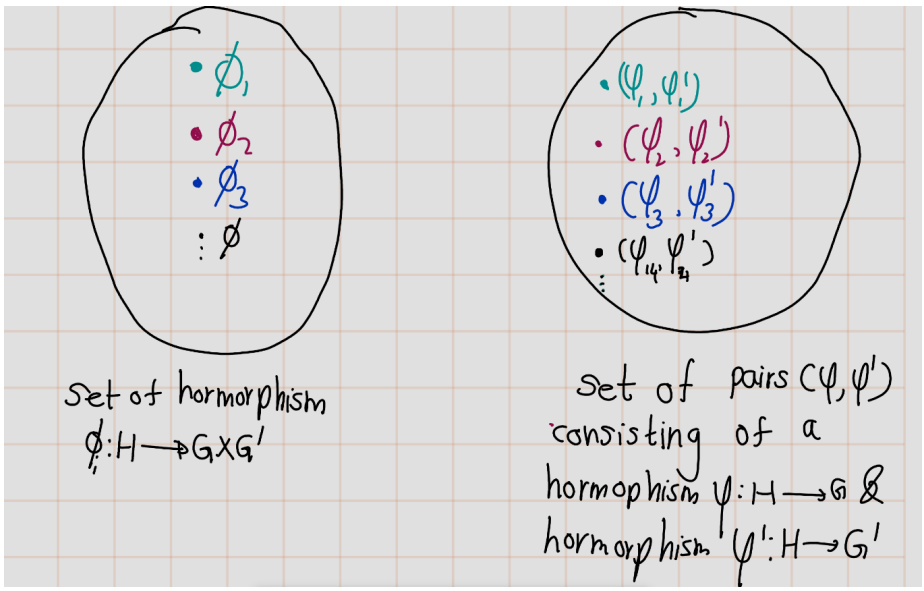
(1) and (2) give contradiction,

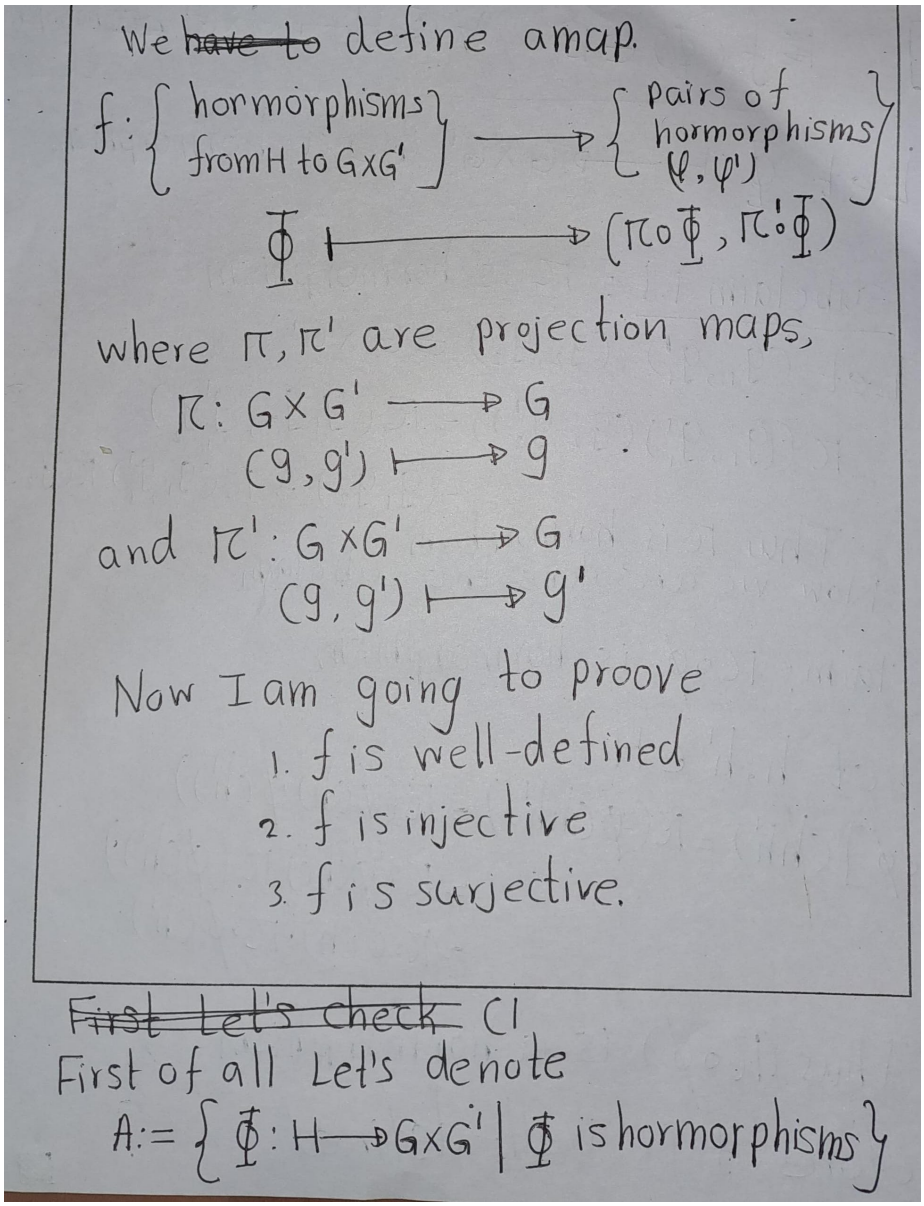
Thus, $H \cap N = \{1\}$

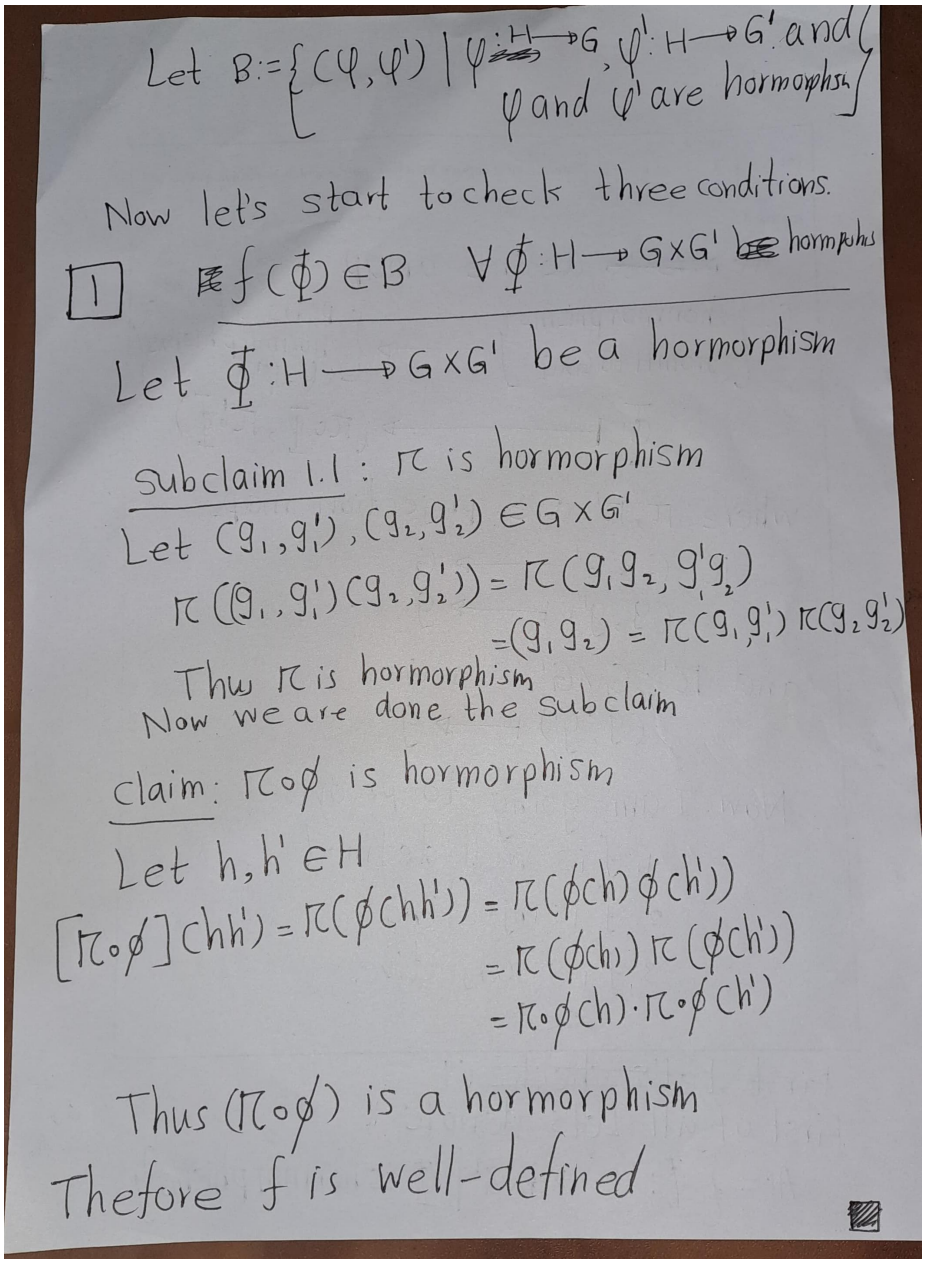
By proposition ~~2.4 cmg~~ (Artins book) 2.11.4 (a), f is injective.



Let G, G', and H be groups. Establish a bijective correspondence between homomorphisms $\phi : H \to G \times G'$ from H to the product group and pairs (φ, φ') consisting of a homomorphism $\varphi : H \to G$ and a homomorphism $\varphi' : H \to G'$.




We ~~have to~~ define amap.
$f: \{\text{hormorphisms from } H \text{ to } G\times G'\} \longrightarrow \{\text{pairs of hormorphisms } (\varphi,\varphi')\}$
$\Phi \longmapsto (\pi\circ\Phi, \pi'\circ\Phi)$
where π, π' are projection maps,
$\pi: G\times G' \longrightarrow G$
$(g,g') \longmapsto g$
and $\pi': G\times G' \longrightarrow G$
$(g,g') \longmapsto g'$
Now I am going to proove
1. f is well-defined
2. f is injective
3. f is surjective.
~~First Let's check~~ C1
First of all Let's denote
$A := \{\Phi: H \longrightarrow G\times G' \mid \Phi \text{ is hormorphisms}\}$



Let $B := \{(\varphi, \varphi') \mid \varphi: H \to G, \varphi': H \to G' \text{ and } \varphi \text{ and } \varphi' \text{ are hormorphsn}\}$

Now let's start to check three conditions.

1 $\exists f(\phi) \in B \quad \forall \phi: H \to G \times G'$ hormphns

Let $\phi: H \to G \times G'$ be a hormorphism

subclaim 1.1 : π is hormorphism

Let $(g_1, g_1'), (g_2, g_2') \in G \times G'$

$$\pi((g_1, g_1')(g_2, g_2')) = \pi(g_1 g_2, g_1' g_2')$$
$$= (g_1 g_2) = \pi(g_1, g_1')\, \pi(g_2 g_2')$$

Thus π is hormorphism
Now we are done the subclaim

claim: $\pi \circ \phi$ is hormorphism

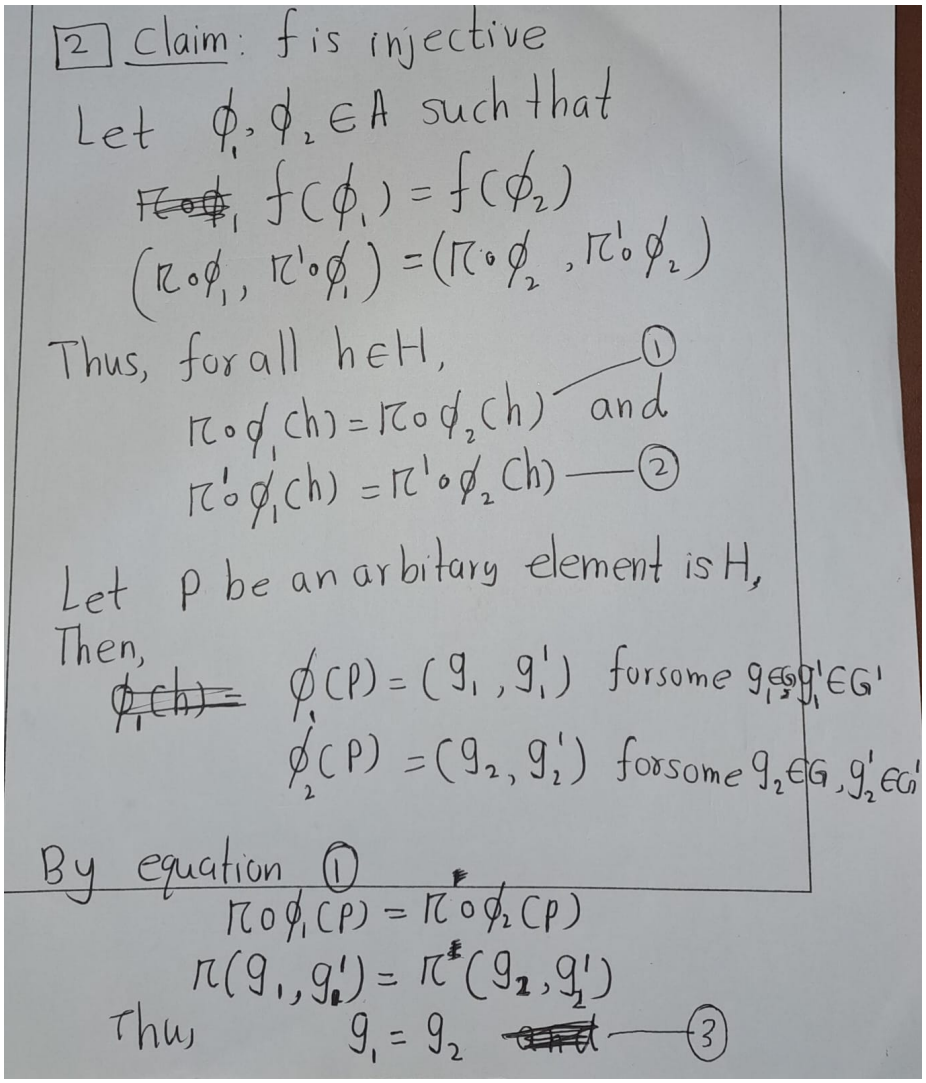
Let $h, h' \in H$

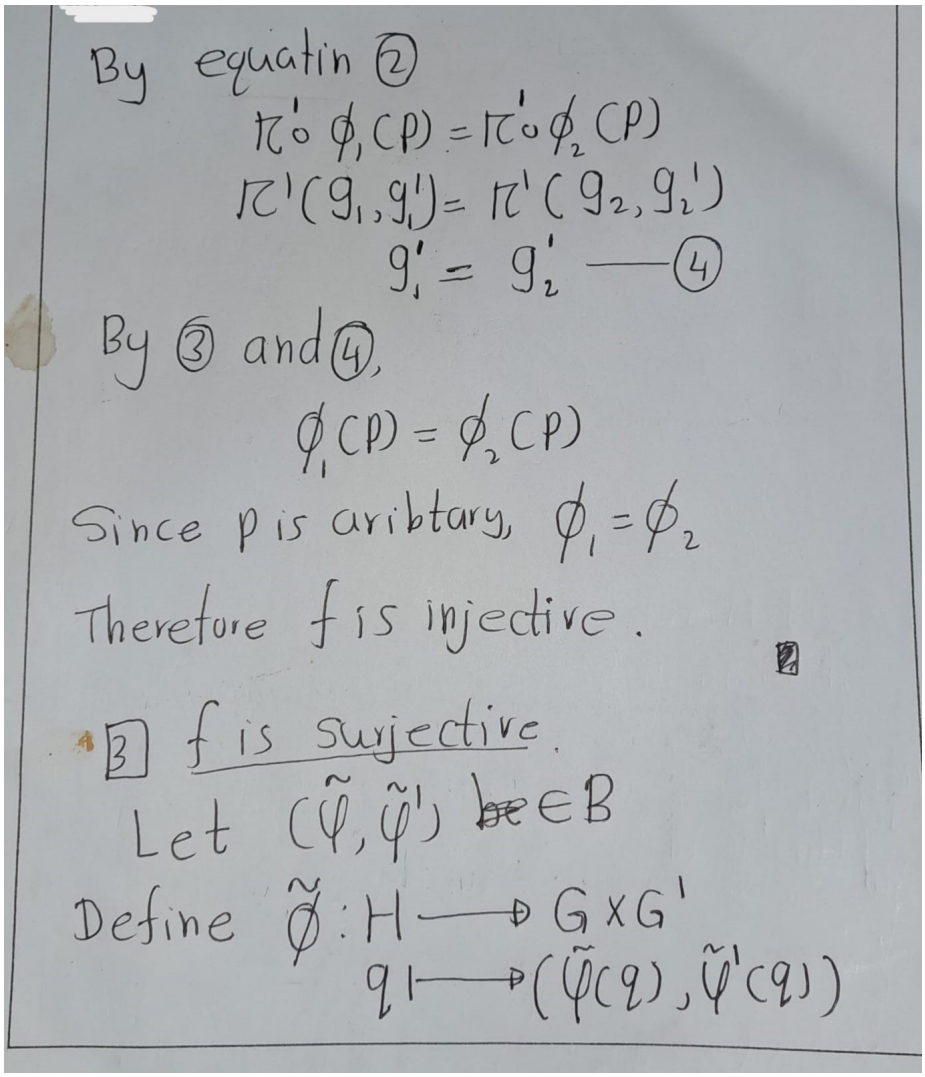
$$[\pi \circ \phi](hh') = \pi(\phi(hh')) = \pi(\phi(h)\phi(h'))$$
$$= \pi(\phi(h))\, \pi(\phi(h'))$$
$$= \pi \circ \phi(h) \cdot \pi \circ \phi(h')$$

Thus $(\pi \circ \phi)$ is a hormorphism

Thefore f is well-defined

∎


2 Claim: f is injective
Let $\phi_1, \phi_2 \in A$ such that
$f(\phi_1) = f(\phi_2)$
$(\pi \circ \phi_1, \pi' \circ \phi_1) = (\pi \circ \phi_2, \pi' \circ \phi_2)$
Thus, for all $h \in H$,
$\pi \circ \phi_1(h) = \pi \circ \phi_2(h)$ and ①
$\pi' \circ \phi_1(h) = \pi' \circ \phi_2(h)$ — ②
Let p be an arbitary element is H,
Then,
$\phi_1(p) = (g_1, g_1')$ forsome $g_1 \in G, g_1' \in G'$
$\phi_2(p) = (g_2, g_2')$ forsome $g_2 \in G, g_2' \in G'$
By equation ①
$\pi \circ \phi_1(p) = \pi \circ \phi_2(p)$
$\pi(g_1, g_1') = \pi(g_2, g_2')$
Thus $g_1 = g_2$ — ③



By equation ②

$$\pi_1' \circ \phi_1(p) = \pi_1' \circ \phi_2(p)$$

$$\pi'(g_1, g_1') = \pi'(g_2, g_2')$$

$$g_1' = g_2' \quad \text{——} ④$$

By ③ and ④,

$$\phi_1(p) = \phi_2(p)$$

Since p is aribtary, $\phi_1 = \phi_2$

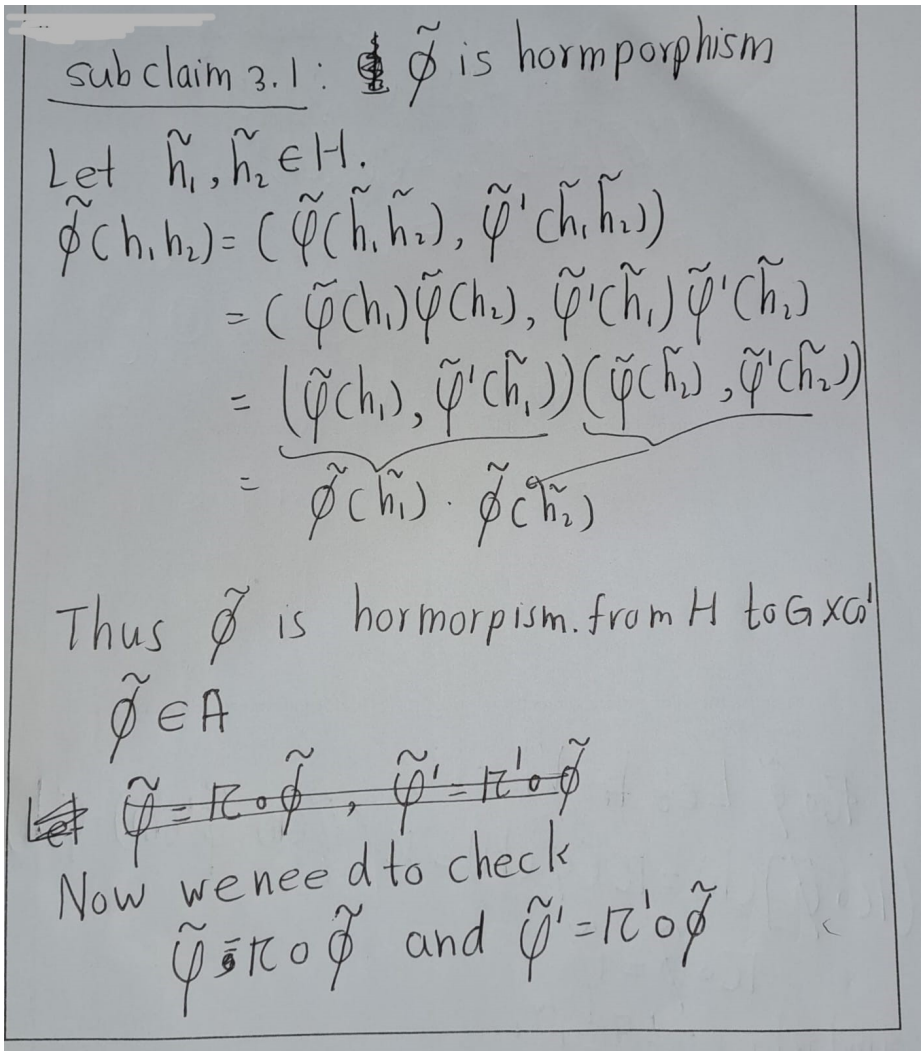
Therefore f is injective. ∎

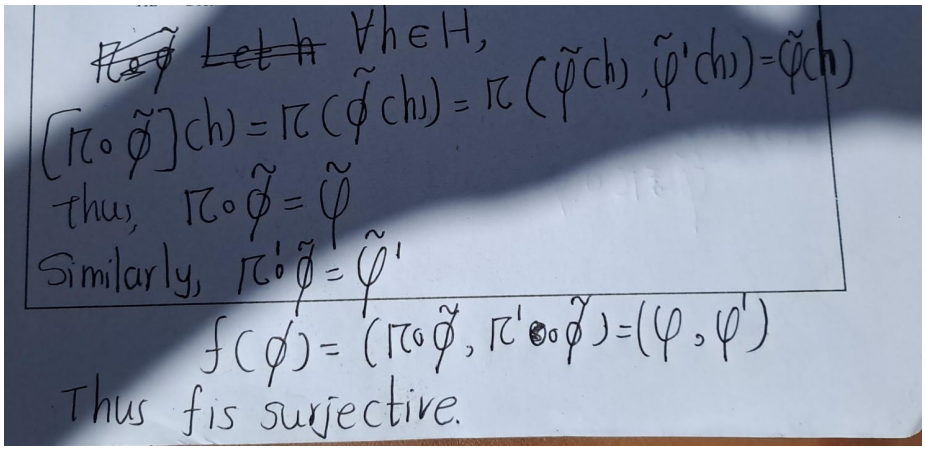
[3] f is surjective.

Let $(\tilde{\varphi}, \tilde{\varphi}') \in B$

Define $\tilde{\phi} : H \longrightarrow G \times G'$

$$q \longmapsto (\tilde{\varphi}(q), \tilde{\varphi}'(q))$$


subclaim 3.1: $\tilde{\phi}$ is hormporphism
Let $\tilde{h}_1, \tilde{h}_2 \in H$.
$\tilde{\phi}(h_1 h_2) = (\tilde{\varphi}(\tilde{h}_1 \tilde{h}_2), \tilde{\varphi}'(\tilde{h}_1 \tilde{h}_2))$
$= (\tilde{\varphi}(h_1)\tilde{\varphi}(h_2), \tilde{\varphi}'(\tilde{h}_1)\tilde{\varphi}'(\tilde{h}_2))$
$= (\tilde{\varphi}(h_1), \tilde{\varphi}'(\tilde{h}_1))(\tilde{\varphi}(\tilde{h}_2), \tilde{\varphi}'(\tilde{h}_2))$
$= \tilde{\phi}(\tilde{h}_1) \cdot \tilde{\phi}(\tilde{h}_2)$
Thus $\tilde{\phi}$ is hormorpism. from H to $G \times G'$
$\tilde{\phi} \in A$
Let $\tilde{\varphi} = \pi \circ \tilde{\phi}$, $\tilde{\varphi}' = \pi' \circ \tilde{\phi}$
Now we need to check
$\tilde{\varphi} = \pi \circ \tilde{\phi}$ and $\tilde{\varphi}' = \pi' \circ \tilde{\phi}$



Let H and K be subgroups of a group G. Prove that the product set HK is a subgroup of G if and only if $HK = KH$.

Solution :

Let G be group and $H, K \leq G$.

- ($\Longrightarrow$): **Claim** : if $HK \leq G$ then $HK = KH$.

  Suppose $HK \leq G$.

  - **sub claim**: Let $x \in KH$. Then $x = kh$ for some $h \in H$ and $k \in K$,

    $$x = kh = 1kh1 = (1k)(h1) \in HK$$

    (Since $1 \in H$ and $1 \in K$). Thus, $KH \subseteq HK$.

  - **sub claim**: $KH \supseteq HK$.
    We can not use previous method.Because we still do not know KH is sub group or not.
    Let $y \in HK$. Since $HK \leq G$, $y^{-1} \in HK$. Then $y^{-1} = hk$ for some $h_0 \in H$ and $k_0 \in K$. \

    $$y = (y^{-1})^{-1} = (h_0k_0)^{-1} = k_0h_0 \in KH$$

    Thus, $KH \supseteq HK$.

Therefore, $KH = HK$.

- ($\Longleftarrow$): **Claim** : If $HK = KH$ then $HK \leq G$.

Now suppose that $HK = KH$.Suppose that $HK = KH$ is empty. Then, H, K is empty. Now we use sub group test.
- *Closure*: Let $x, y \in HK$. Then $x = h_1k_1$ and $y = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$.

$$\begin{aligned} xy &= (h_1k_1)(h_2k_2) && (85)\\ &= h_1(k_1h_2)k_2) \text{ (By associavity property)} && (86)\\ &= h_1(h_3k_3)k_2) \text{ for some } h_3 \in H \text{ and } k_3 \in K \text{ (Since} KH = HK) && (87)\\ &= (h_1h_3)(k_3k_2) \in HK && (88) \end{aligned}$$

- *Inverse*: Let Let $x \in HK$. Then $x = h'k'$ for some $h' \in H$ and $k' \in K$.

$$x^{-1} = (h'k')^{-1} = k'h' \in KH = HK$$

Thus, $HK \leq G$.

Therefore, the product set HK is a subgroup of G if and only if $HK = KH$

Quotient Groups

Show that if a subgroup H of a group G is not normal, there are left cosets aH and bH whose product is not a coset.

Suppose that $H \leq G$ but $H \not\trianglelefteq G$. We are going to use indirect proof. So, assume that $(aH)(bH)$ is a coset for all $a, b \in G$. Then,

$$aHbH = abH$$

then for all $h_1, h_2, h_3 \in H$, So,

$$ah_1bh_2 = abh_3$$

$$\begin{aligned} ah_1bh_2 &= abh_3 && (89)\\ a^{-1}(ah_1bh_2) &= a^{-1}(abh_3) && (90)\\ (a^{-1}a)(h_1bh_2) &= (a^{-1}a)(bh_3) && (91)\\ h_1bh_2 &= bh_3 && (92)\\ b^{-1}(h_1bh_2)h_2^{-1} &= b^{-1}(bh_3)h_2^{-1} && (93)\\ b^{-1}h_1b(h_2h_2^{-1}) &= (b^{-1}b)h_3h_2^{-1} && (94)\\ b^{-1}h_1b &= h_3h_2^{-1} \in H && (95)\\ & && (96) \end{aligned}$$

Thus, $b^{-1}h_1b \in H$. and since $b \in G$ and $h_1 \in H$ is arbitary, H is normal subgroup, which contradict the our hypothesis. Thus, there exist left cosets aH and bH whose product is not a coset.

In the general linear group $GL_3(\mathbb{R})$, consider the subsets:

$$H = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \mid * \text{ represents an arbitrary real number} \right\}$$

and

$$K = \left\{ \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid * \text{ represents an arbitrary real number} \right\}$$

Show that H is a subgroup of GL_3, that K is a normal subgroup of H, and identify the quotient group H/K. Determine the center of H.

- **Claim 1**: $H \leq G$.
  Certainly! Let's prove that the subset H is a subgroup of the general linear group $GL_3(\mathbb{R})$.
  - *Non-emptiness*: We start by showing that H is non-empty. The identity matrix $\mathbf{I}_3$ belongs to H since it satisfies the conditions for H:
    $$\mathbf{I}_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
    Therefore, H is non-empty.
  - *Closure under matrix multiplication*: Let $\mathbf{A}$ and $\mathbf{B}$ be matrices in H. We need to show that their product $\mathbf{AB}$ is also in H. Consider:
    $$\mathbf{A} = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$$
    The product $\mathbf{AB}$ is:
    $$\mathbf{AB} = \begin{pmatrix} 1 & a+x & by+az+b \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{pmatrix}$$
    ““‘ Since $a + x$, $y + az + b$, and $c + z$ are arbitrary real numbers, $\mathbf{AB}$ satisfies the conditions for H. Hence, H is closed under matrix multiplication.
  - *Closure under taking inverses*: Let $\mathbf{A}$ be a matrix in H. We need to show that its inverse $\mathbf{A}^{-1}$ is also in H. The inverse of $\mathbf{A}$ is:

$$\mathbf{A}^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$$

Again, since $-a$, $ac-b$, and $-c$ are arbitrary real numbers, $\mathbf{A}^{-1}$ satisfies the conditions for H. Therefore, H is closed under taking inverses. Hence, we have shown that H is a subgroup of $GL_3(\mathbb{R})$.

- **Claim 2** : $K \leq H$.
  I am not going to prove that this case, because this is exhausting. This is very easy.
- **Claim 3** : K is normal sub group of H.
  Let $A := \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \in H$ and $B := \begin{bmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in K$, where $a, b, c, d \in \mathbb{R}$.
  Then,

$$\begin{aligned} ABA^{-1} &= \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix} && (97) \\ &= \begin{bmatrix} 1 & a & d+b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix} && (98) \\ &= \begin{bmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in K && (99) \end{aligned}$$

Thus, K is normal sub group of H.

- **Quotient group** H/K :
  Let $h_1, h_2 \in H$ be such that

$$h_1 = \begin{bmatrix} 1 & a_1 & b_1 \\ 0 & 1 & c_1 \\ 0 & 0 & 1 \end{bmatrix} \text{ and } h_2 = \begin{bmatrix} 1 & a_2 & b_2 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{bmatrix}.$$

  Suppose that $h_1K = h_2K$. By Artin's book 2.85, $h_1^{-1}h_2 \in K$.

$$h_1^{-1}h_2 = \begin{bmatrix} 1 & -a_1 & a_1c_1 - b_1 \\ 0 & 1 & -c_1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a_2 & b_2 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -a_1+a_2 & b_2 - a_1c_2 + a_1c_1 - b_1 \\ 0 & 1 & -c_1+c_2 \\ 0 & 0 & 1 \end{bmatrix}$$

  Since,

$$h_1K = h_2K \iff h_1^{-1}h_2 \in K \tag{100}$$
$$\iff -a_1 + a_2 = 0 \text{ and } -c_2 - c_1 \tag{101}$$
$$\iff a_1 = a_2 \text{ and } c_1 = c_2 \tag{102}$$

Thus,

$$H/K = \left\{ hK \middle| \begin{bmatrix} 1 & a & 0 \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}, a, c \in \mathbb{R} \right\}$$

- **Center of Group H**

$$Z(H) = \left\{ A \in H \middle| AX = XA \text{ for all } X \in H \right\}$$

Let's find center. We need to find $a, b, c \in \mathbb{R}$ such that

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \text{ for all } x, y, z \in \mathbb{R} \tag{103}$$

$$\begin{bmatrix} 1 & a+x & b+y+az \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+x & b+y+xc \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{bmatrix} \tag{104}$$

By comparing 1×3 index, we need to find that $a, b, c \in \mathbb{R}$ $az = xc$ for all $x, y, z\mathbb{R}$. SO, the only possibility is $a = c = 0$. Thus,

$$Z(H) = \left\{ \begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \middle| b \in \mathbb{R} \right\}$$

Let P be a partition of a group G with the property that for any pair of elements A, B of the partition, the product set AB is contained entirely within another element C of the partition. Let N be the element of P that contains 1. Prove that N is a normal subgroup of G and that P is the set of its cosets.

- **Claim 1**: The product set $NN = N$.
  Let $x \in N$, Then $x = x \cdot 1 \in NN$. Thus, $N \subseteq NN$. We know that the product set NN is contained entirely within in an element of pratition, but N is a partion. The only way this happen $N = NN$.
- **Claim 2**: $N \leq G$.
  - *Subset*: It is very clear that $N \subseteq G$.

- *Closure*: Let $x, y \in N$. Then $(xy) \in NN = N$. So, N is closed under composition.
- *Identity*: Given that $1 \in N$.
- *Inverse*: Let $x \in N$. We have to show that x^{-1} is contained in N. We use proof by contardiction. So, Assume contary, $x^{-1} \in M$, M is an elemenet of partion P such that $N \neq M$.

$$xx^{-1} \in NM, xx^{-1} = 1 \in N$$

So, we would have $NM \subseteq N$ (since the product set is contained entirely wiithin one of the sets of partition). On the other hand,

$$1x^{-1} \in NM, 1x^{-1} = x^{-1} \in N$$

So, $NM \subseteq N$a contradiction.

Therefore, conclude that our assumption that $x^{-1} \notin N$ was wrong, that we must have $x^{-1} \in N$

- **Claim 3**: $N \trianglelefteq$
  Let $a \in G$ and $n \in N$. Let $a \in A$ and $a^{-1} \in B$, where $A, B \in P$.

  $$ana^{-1} = ANB$$

  , But also, $1 \in N$,

  $$g \cdot 1 \cdot g^{-1} = 1 \in ANB$$

  Since P spilts into disjoint subsets and the only one element of partion that containn 1 is N.

  $$ANB = N$$

  and but also $gng^{-1} \in N$. Thefeore, N is normal sub group.

-**Claim 4**: P is the set of its cosets.
Let A be some element Of partition, and let $a \in A$.

Need to prove: $A = aN$

- Subclaim 4.1: $A \subseteq aN$.
  Let $a \in A$. Let $b \in B$, where B is elmenet of partion. Then $b^{-l}b \in BA$, $b^{-l} = 1 \in N$ So, $BA \subseteq N$. Specially,

  $$b^{-1}a \in N$$

  So there exists some $n \in N$ such that

  $$b^{-1}a = n \quad \iff \quad a = bn \quad \iff \quad b = an^{-1}$$

  Since $N \leq G$. $n^{-1} \in N$. Thus, $b \in aN$, so $A \subset aN$.

- Subcliam 4.2 : $A \supseteq aN$.

  - subclaim 4.2.1: $AN \subseteq A$,

Note that $a \in A$ and $1 \in N$, Thus,

$$a \cdot 1 \in AN, \quad a \cdot 1 = a \in A$$

Since, the product set is contained entirely in one element partition. Thus, $AN \subseteq A$

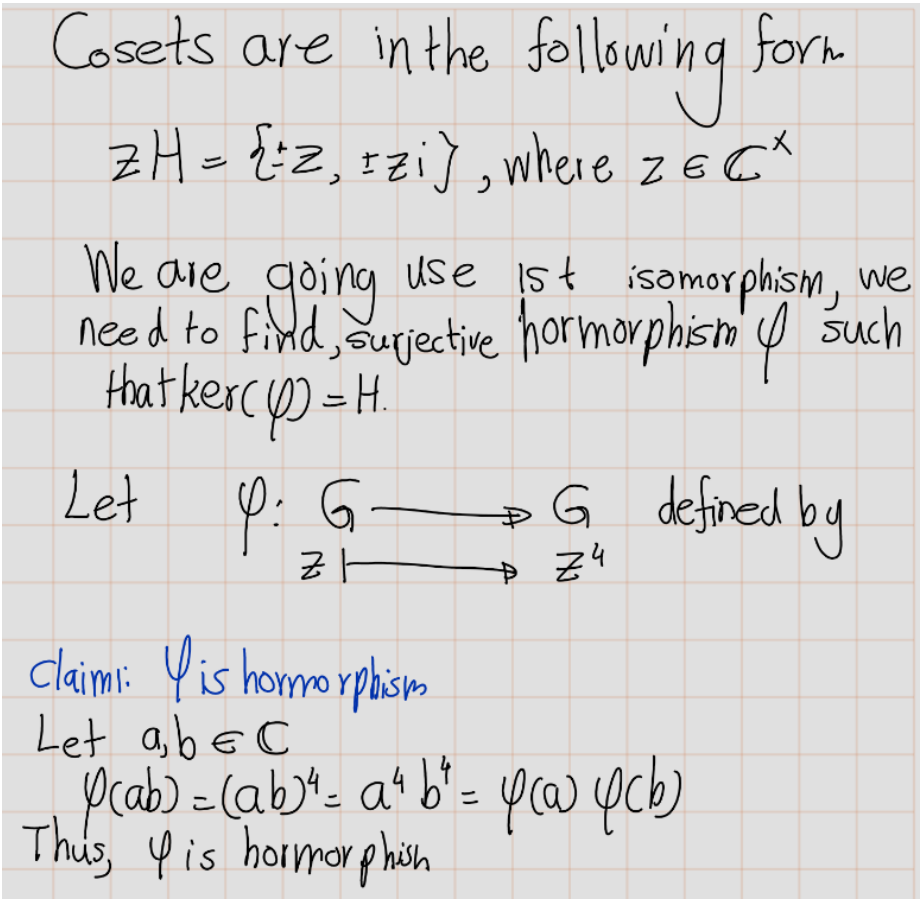
Now,

$$aN = \{an | n \in N\} \subseteq \{an : a \in A, n \in N\} = AN \subseteq A$$

Thus, $ax \in A$, as required. Thus $aN \subseteq A$

Hence, we can conclude that $A = aN$.

Let $H = \{\pm 1, \pm i\}$ be the subgroup of $G = C^{\times}$ of fourth roots of unity. Describe the cosets of H in G explicitly. Is G/H isomorphic to G?



Claim 2: φ is surjective.

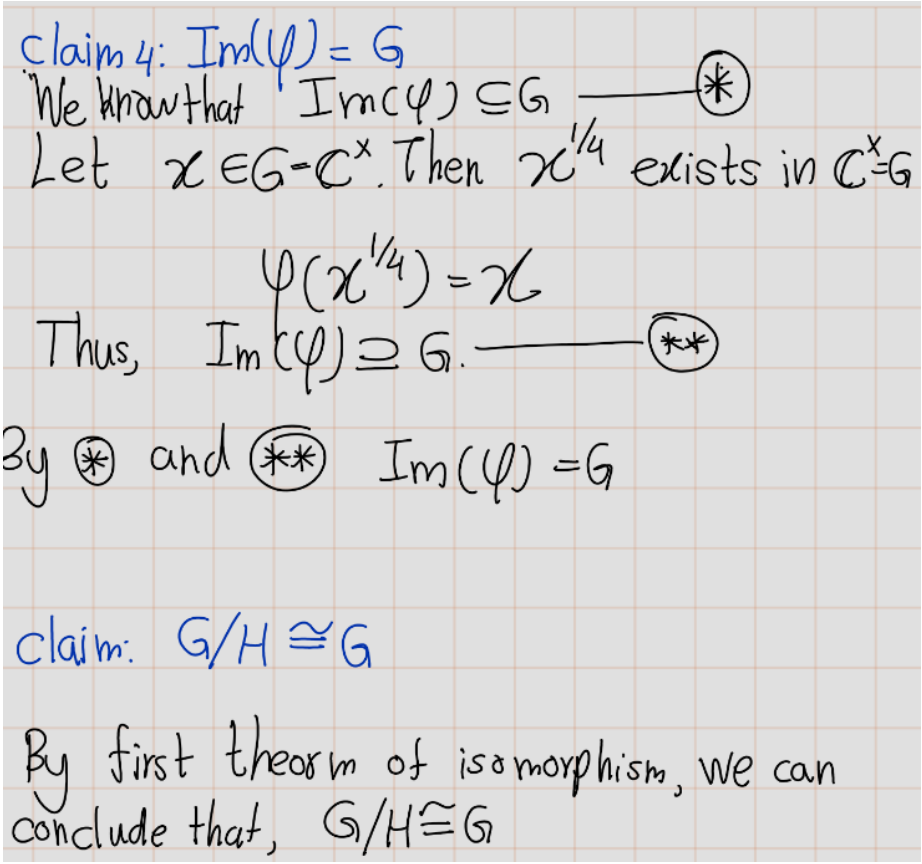
Let $c \in G$. Then let $d = \sqrt[4]{c}$.
We know that d is exist. Because $\mathbb{C}^\times$ have all nth roots every element of $\mathbb{C}^\times$ (algebrically closed.). Then,

$$\varphi(d) = c$$

Thus, φ is surjective.

Claim 3: $\ker(\varphi) = H$

$$\begin{aligned}
\ker(\varphi) &= \{x \mid x^4 = 1\} \\
&= \{e^{\frac{2\pi i k}{4}} \mid k = 0, 1, 2, 3\} \\
&= \{e^0, e^{\frac{2\pi i}{4}}, e^{\frac{4\pi i}{4}}, e^{\frac{6\pi i}{4}}\} \\
&= \{e^0, e^{\pi i/2}, e^{\pi i}, e^{3\pi i/2}\} \\
&= \{1, i, -1, -i\} \\
&= H
\end{aligned}$$



Let G be the group of upper triangular real matrices $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ with a and d different from zero. For each of the following subsets, determine whether or not S is a subgroup, and whether or not S is a normal subgroup. If S is a normal subgroup, identify the quotient group G/S.

1. S is the subset defined by $b = 0$.
2. S is the subset defined by $d = 1$.
3. S is the subset defined by $a = d$.

(i) $S_1 := \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} : a, b \in \mathbb{R} \setminus \{0\} \right\}$

Observe that $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S_1$. Thus, $S \neq \emptyset$

Let $A, B \in G$. Then

$A := \begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix}$ for some $a_1, a_2, b_1, b_2 \in \mathbb{R} \setminus \{0\}$

$B := \begin{bmatrix} b_1 & 0 \\ 0 & b_2 \end{bmatrix}$

Then $B^{-1} = \frac{1}{b_1 b_2} \begin{bmatrix} b_2 & 0 \\ 0 & b_1 \end{bmatrix} = \begin{bmatrix} 1/b_1 & 0 \\ 0 & 1/b_2 \end{bmatrix}$

So, $B^{-1} \in G$. Thus,

$$AB^{-1} = \begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix} \begin{bmatrix} 1/b_1 & 0 \\ 0 & 1/b_2 \end{bmatrix} = \begin{bmatrix} a_1/b_1 & 0 \\ 0 & a_2/b_2 \end{bmatrix}$$

Since $\frac{a_1}{b_1}, \frac{a_2}{b_2} \in \mathbb{R} \setminus \{0\}$, Thus $AB^{-1} \in S$

Therefore, S is a subgroup.

Let's check S_1 is normal or not

Claim: S_1 is not normal

Let $X := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in G$. Then

$X^{-1} := \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$

Let $Y := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \in B$. Then,

$XYX^{-1} = \begin{bmatrix} 1 & -2 \\ 0 & -1 \end{bmatrix}$. But $XYX^{-1} \notin B$

Therefore, B is NOT a Normal subgroup

② $S'' := \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a, b \in \mathbb{R} \right\}$

claim: $S'' \leq G$

Observe that $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S''$. Thus $S'' \neq \emptyset$.

Let $X'' := \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$ & $Y'' := \begin{bmatrix} e & f \\ 0 & 1 \end{bmatrix} \in S''$

Then $(Y'')^{-1} := \frac{1}{e} \begin{bmatrix} 1 & -f \\ 0 & e \end{bmatrix}$

$= \begin{bmatrix} 1/e & -f/e \\ 0 & 1 \end{bmatrix}$

$(X'')(Y'')^{-1} := \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1/e & -f/e \\ 0 & 1 \end{bmatrix}$

$= \begin{bmatrix} ae & af+b \\ 0 & 1 \end{bmatrix} \in S''$

Thus, $S'' \leq G$

Cosets

Let $gS, hS \in G/S$.

$$gS = hS \iff h^{-1}g \in S$$

Let $g := \begin{bmatrix} g_1 & g_2 \\ 0 & g_3 \end{bmatrix}$, $h := \begin{bmatrix} h_1 & h_2 \\ 0 & h_3 \end{bmatrix}$

where, $g_1, g_2, g_3, h_1, h_2, h_3 \in \mathbb{R}$ and $g_1, g_2, h_1 h_3 \neq 0$

Then, $h^{-1}g = \begin{bmatrix} 1/h_1 & -h_2/h_1 h_3 \\ 0 & 1/h_3 \end{bmatrix} \begin{bmatrix} g_1 & g_2 \\ 0 & g_3 \end{bmatrix}$

$$= \begin{bmatrix} g_1/h_1 & g_2/h_1 - \frac{g_2 h_2}{h_1 h_3} \\ 0 & g_3/h_3 \end{bmatrix}$$

Thus $h^{-1}g \in S \iff \frac{g_3}{h_3} = 1 \iff g_3 = h_3$

Therefore, $gS \neq hS \iff g_3 \neq h_3$

Note that g_1, g_2 does not help to determine whether two cosets are equal. Thus, we can fix $a=1$, $b=0$,

$$G/S := \left\{ gS \mid g = \begin{bmatrix} 1 & 0 \\ 0 & c \end{bmatrix}, c \in \mathbb{R} \setminus \{0\} \right\}$$

③ $S''' := \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} : a, b \in \mathbb{R}, a \neq 0 \right\}$

Observe that, $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S'''$. Thus, $S''' \neq \emptyset$

Let $A := \begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$ $B := \begin{bmatrix} e & f \\ 0 & e \end{bmatrix} \in S'''$, where $a, b, e, f \in \mathbb{R}$ & $a \neq 0 \neq e$

Then $B^{-1} = \frac{1}{e^2} \begin{bmatrix} e & f \\ 0 & e \end{bmatrix} = \begin{bmatrix} 1/e & -f/e \\ 0 & 1/e \end{bmatrix}$

$$AB^{-1} = \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \begin{bmatrix} 1/e & -f/e \\ 0 & 1/e \end{bmatrix} = \begin{bmatrix} ae & af+be \\ 0 & ae \end{bmatrix} \in S'''$$

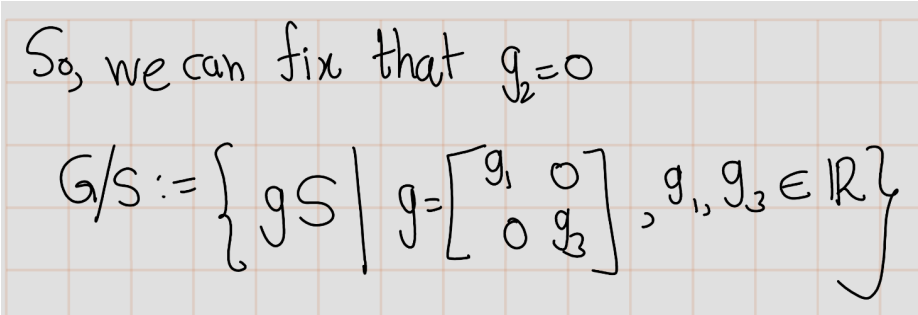
Thus, $S''' \leq G$

Let $A := \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in G$. So, $A^{-1} := \begin{bmatrix} 1/a & -b \\ 0 & -1/c \end{bmatrix}$

Let $B := \begin{bmatrix} e & f \\ 0 & e \end{bmatrix} \in S'''$. Then

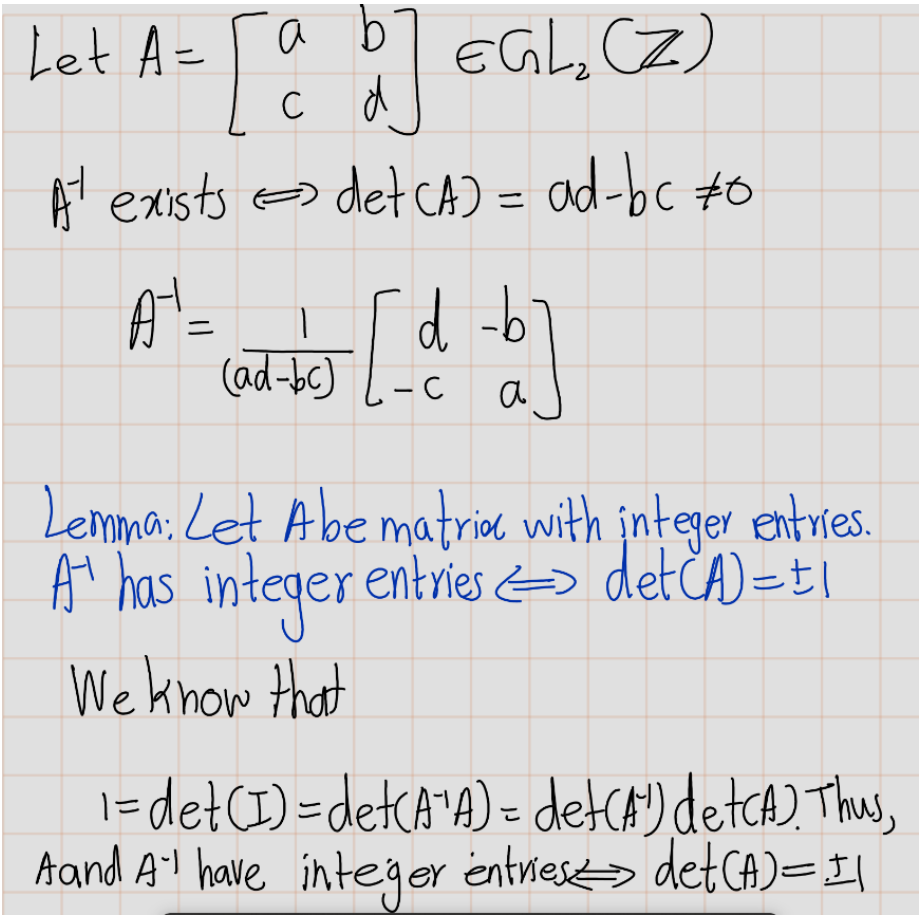
$$ABA^{-1} = \begin{bmatrix} e & \frac{(eb+af+be)}{a} \\ 0 & e \end{bmatrix} \in S'''$$

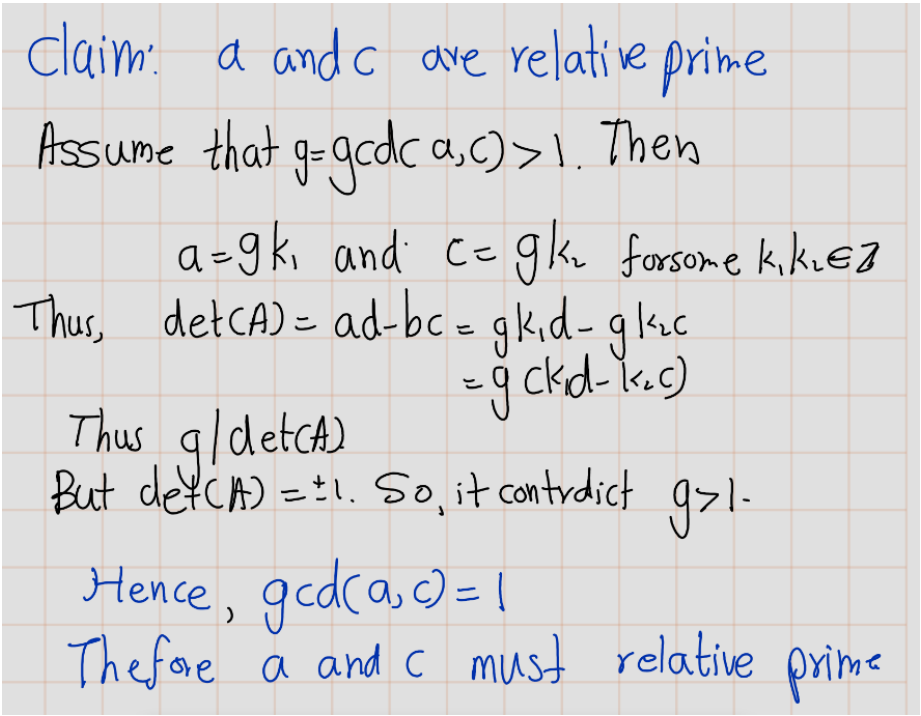
Thus, S''' is normal.



Miscellaneous Problems

Describe the column vectors $(a, c)^T$ that occur as the first column of an integer matrix A whose inverse is also an integer matrix.





(a) Prove that every group of even order contains an element of order 2.
(b) Prove that every group of order 21 contains an element of order 3.

Claim a : Let G be a group whose identity is e.Let G be of even order.Then,$\exists x \in G : |x| = 2$

(Claim a) In any group G, the identity element e is self-inverse with the property that the identity is the only group element of order 1, and is the only such element.

That leaves an odd number of elements.

Each element in $x \in G : |x| > 2$ can be paired off with its inverse, as $|x^{-1}| = |x| > 2$ (Since order of a group element equals the order of its inverse.)

Hence there must be at least one element which has not been paired off with any of the others which is therefore self-inverse. Let's say it , $'y'$.

$$y^{-1} = y \iff x \cdot y = e \tag{105}$$
$$\iff |y| = 2 \tag{106}$$

Thus, every group of even order contains an element of order 2.

Claim b: Let G be a group whose identity is e.Let G be of order 21.(|G=21|) Then,$\exists x \in G : |x| = 3$

Problem

Vector spaces.