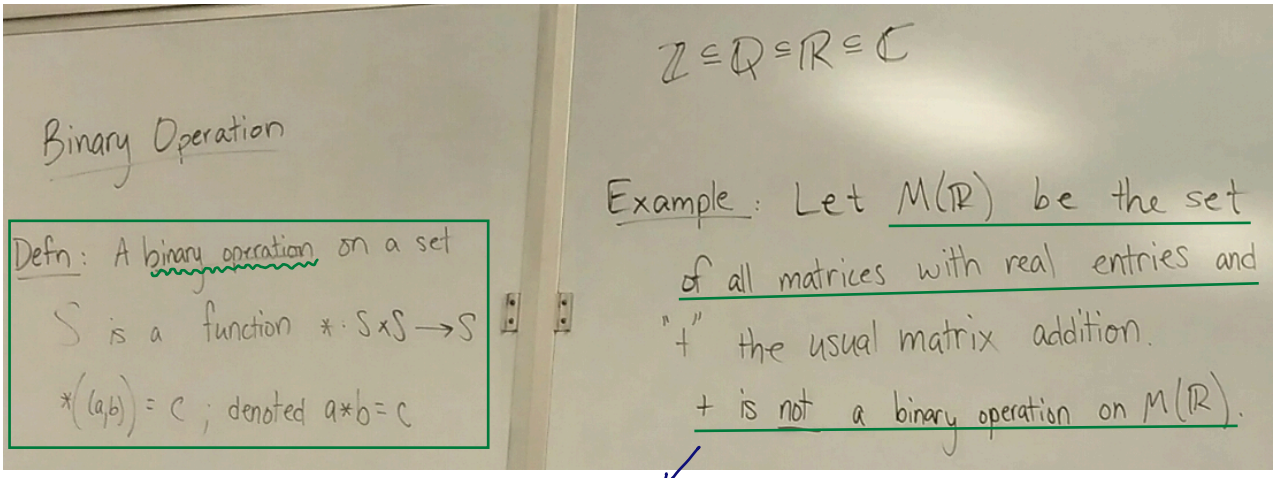
SOORAJ SOMAN | **Math 5105 Modern Algebra Notes**
Student ID: 12617667, Computer Science, Missouri S&T
Rolla, MO, USA | Phone: 573 537 0671, +91 9400635788
ss4kx@umsystem.edu | soorajss1729@gmail.com

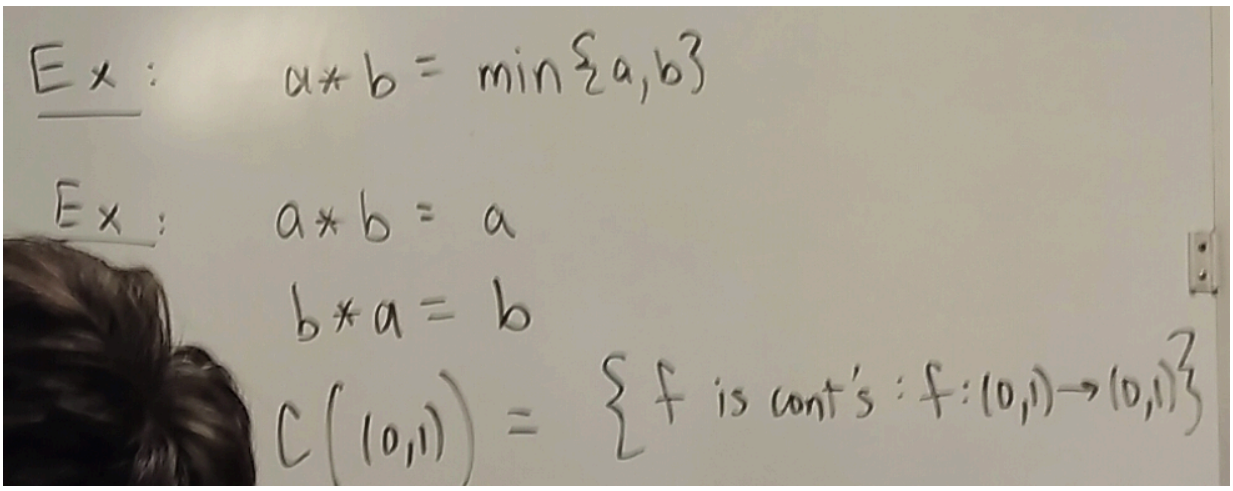


because $A+B$ is not defined for an ordered pair (A,B) of matrices having different # of rows or of columns.

- we require a binary operation on a set S to be defined for *every* ordered pair (a, b) of elements from S.

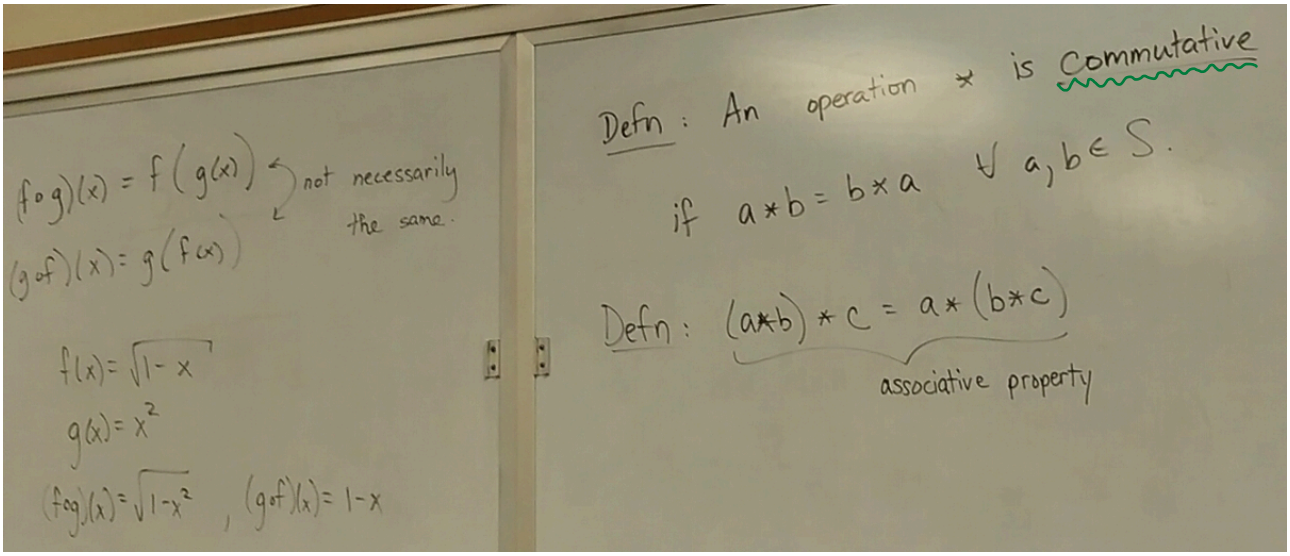
Let $*$ be a binary operation on S and let H be a subset of S. The subset H is **closed under** $*$ if for all $a, b \in H$ we also have $a * b \in H$. In this case, the binary operation on H given by restricting $*$ to H is the **induced operation** of $*$ on H. ■

$\Rightarrow$ $*$ is the induced binary operation on H.

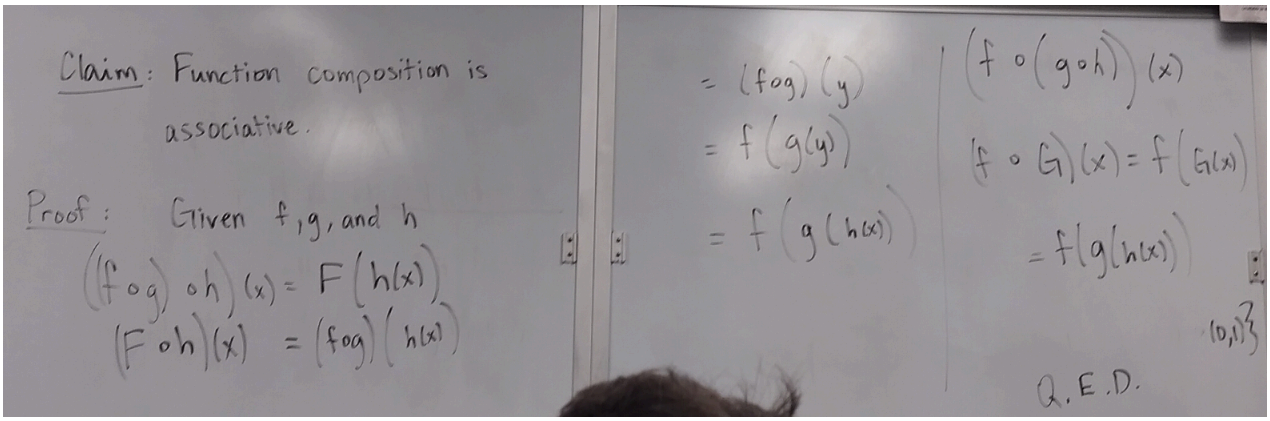


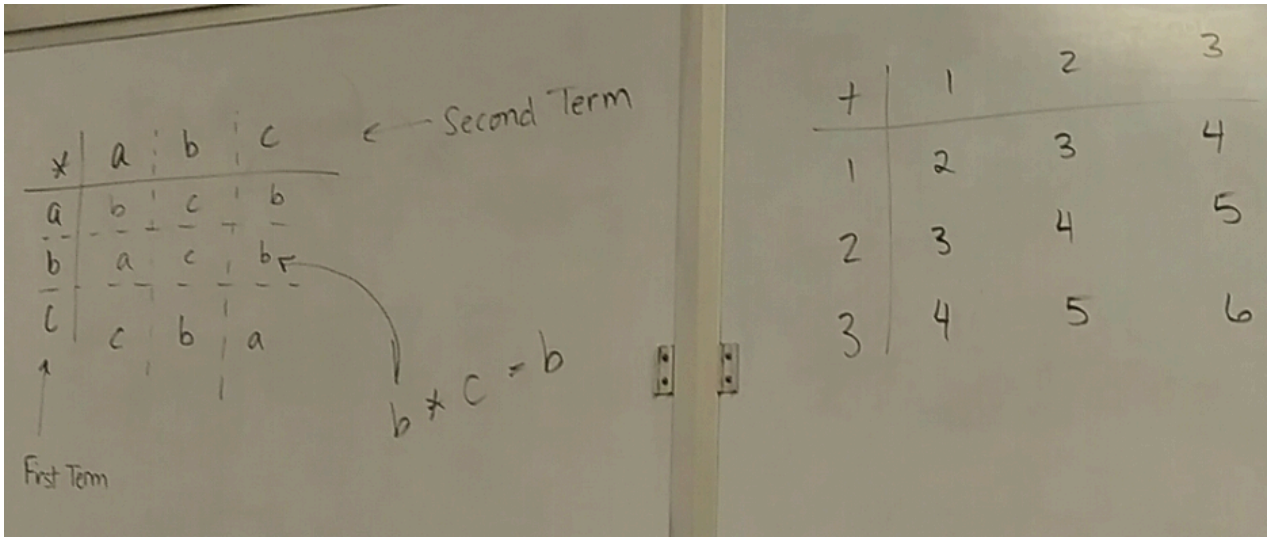
$+$ is not an induced binary operation on $\mathbb{R}^*$
because $2 \in \mathbb{R}, -2 \in \mathbb{R}$ but $-2+2=0 \notin \mathbb{R}^*$

$*$ such that $a*b = a/b$ is not a binary operation for $\mathbb{Q}$



A binary operation on a set S is **associative** if $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.





1. *exactly one element is assigned to each possible ordered pair of elements of* S,
2. *for each ordered pair of elements of* S, *the element assigned to it is again in* S.

On $\mathbb{Q}$, let $a * b = a/b$. Here $*$ is *not everywhere defined* on $\mathbb{Q}$, for no rational number is assigned by this rule to the pair (2, 0). ▲

On $\mathbb{Q}^+$, let $a * b = a/b$. Here both Conditions 1 and 2 are satisfied, and $*$ is a binary operation on $\mathbb{Q}^+$. ▲

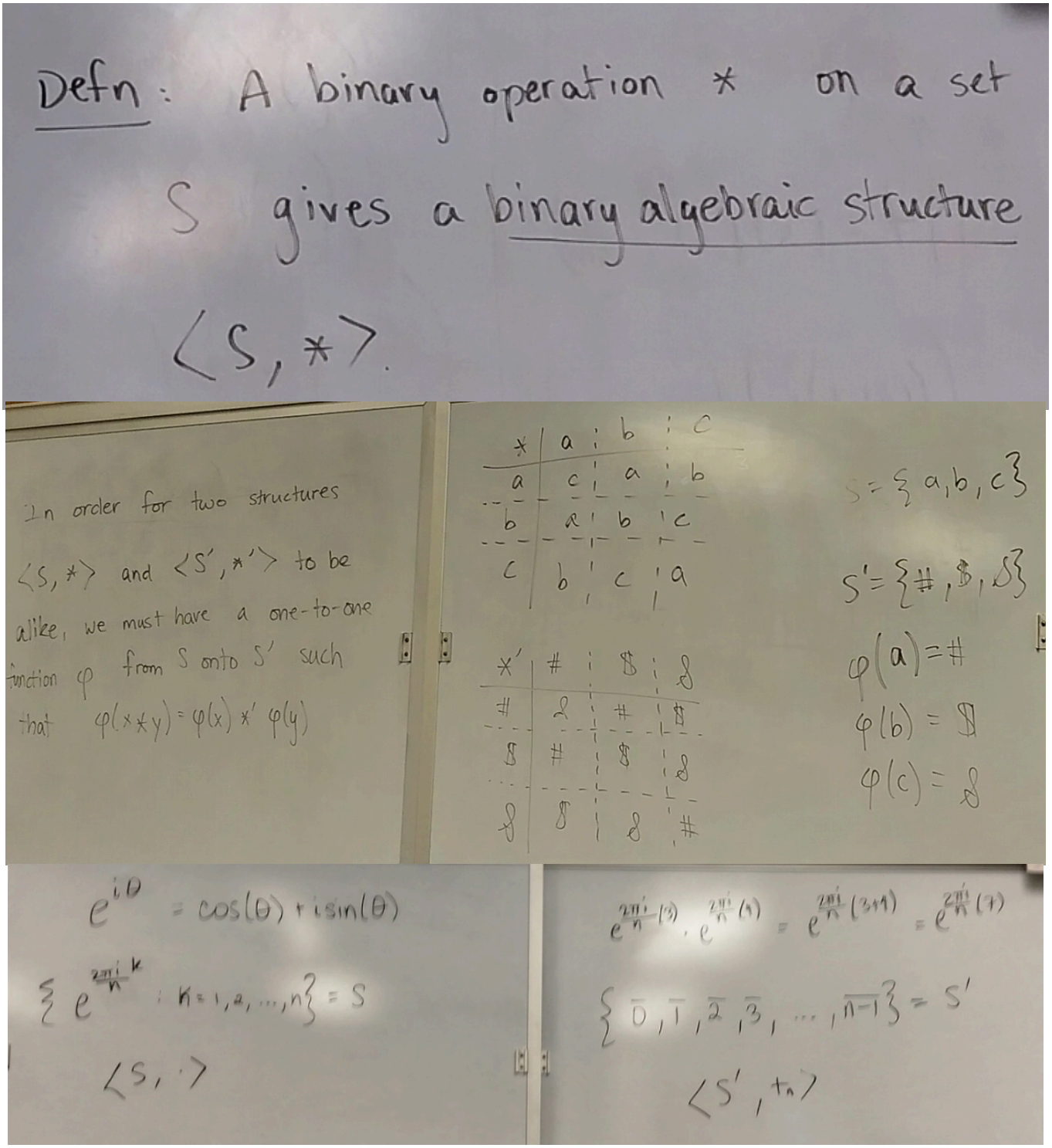
On $\mathbb{Z}^+$, let $a * b = a/b$. Here Condition 2 fails, for $1 * 3$ is not in $\mathbb{Z}^+$. Thus $*$ is not a binary operation on $\mathbb{Z}^+$, since $\mathbb{Z}^+$ is *not closed under* $*$. ▲

Let F be the set of all real-valued functions with domain $\mathbb{R}$ as in Example 2.7. Suppose we "define" $*$ to give the usual quotient of f by g, that is, $f * g = h$, where $h(x) = f(x)/g(x)$. Here Condition 2 is violated, for the functions in F were to be defined for *all* real numbers, and for some $g \in F$, $g(x)$ will be zero for some values of x in $\mathbb{R}$ and $h(x)$ would not be defined at those numbers in $\mathbb{R}$. For example, if $f(x) = \cos x$ and $g(x) = x^2$, then $h(0)$ is undefined, so $h \notin F$. ▲

Let F be as in Example 2.22 and let $f * g = h$, where h is the function greater than both f and g. This "definition" is completely worthless. In the first place, we have not defined what it means for one function to be greater than another. Even if we had, any sensible definition would result in there being many functions greater than both f and g, and $*$ would still be *not well defined.* ▲

Let S be a set consisting of 20 people, no two of whom are of the same height. Define $*$ by $a * b = c$, where c is the tallest person among the 20 in S. This is a perfectly good binary operation on the set, although not a particularly interesting one. ▲

Let S be as in Example 2.24 and let $a * b = c$, where c is the shortest person in S who is taller than both a and b. This $*$ is *not everywhere defined,* since if either a or b is the tallest person in the set, $a * b$ is not determined. ▲



Let $\langle S, * \rangle$ and $\langle S', *' \rangle$ be binary algebraic structures. An **isomorphism of** S with S' is a one-to-one function ϕ mapping S onto S' such that

$$\phi(x * y) = \phi(x) *' \phi(y) \text{ for all } x, y \in S.$$

homomorphism property

There exists a function $\phi: S \to S'$ such that
- ϕ is one-to-one
- ϕ is onto
- $\phi(x*y) = \phi(x) *' \phi(y) \quad \forall x, y \in S$ (homomorphism property)

If such a map ϕ exists, then S and S' are **isomorphic binary structures**, which we denote by $S \simeq S'$, omitting the $*$ and $*'$ from the notation. ■

A binary structure is "the same" same structure as another if

(1) there is a one-to-one function.
(2) the function is onto
(3) $f(x * y) = f(x) *' f(y)$

Homomorphism property

A function between S and S' satisfying these three conditions are called isomorphisms.

$f: \langle U_n, \cdot \rangle \longrightarrow \langle \mathbb{Z}/n\mathbb{Z}, + \rangle$

$f(e^{\frac{(2\pi i)}{n}k}) = \bar{k}$ is an isomorphism

Defn: A structural property of a binary structure is a prop. that is shared by all isomorphic structures.

(1) Cardinality of the sets
(2) Solutions to equations
(3) Operation is commutative

Note: Let the equation $a * x = b$ is in $\langle S, * \rangle$ where $a, b, x \in S$.

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

$\Rightarrow$ If x is a solution to the eq^n. $a * x = b$ in $\langle S, * \rangle$, then $\phi(x)$ is a solution to the eq^n. $\phi(a) *' y = \phi(b)$ in $\langle S', *' \rangle$ where $y = \phi(x)$.

Defn: The identity of an algebraic structure $\langle S, * \rangle$ is an element e such that

$e * x = x * e = x$

Theorem: If a binary structure has an identity element, then that element is unique.

Proof: Let $\langle S, * \rangle$ be the structure and suppose e and e' satisfy $x * e = e * x = x$, $x * e' = e' * x = x$ for all $x \in S$.

$e = e * e' = e'$

$\Rightarrow e = e'$

Q.E.D.

Theorem: Suppose $\langle S, * \rangle$ has an identity element e. If $\varphi: S \to S'$ is an isomorphism of $\langle S, * \rangle$ with $\langle S', *' \rangle$, then $\varphi(e)$ is an identity element of S'.

Proof: Let $s' \in S'$

Goal: $\varphi(e) *' s' = s' *' \varphi(e) = s'$

$s' \in \text{range}(\varphi) \Rightarrow \varphi(s) = s'$

$\varphi(e) *' \varphi(s) = \varphi(e * s) = \varphi(s * e)$

$= \varphi(s) \quad = \varphi(s) *' \varphi(e)$

$= s' \quad = s' *' \varphi(e)$

$\Longrightarrow$

Thus, $\varphi(e)$ satisfies the conditions of an identity element in S'.

Q.E.D.

GROUPS

A **group** $\langle G, * \rangle$ is a set G, closed under a binary operation $*$, such that the following axioms are satisfied:

$\mathscr{G}_1$: For all $a, b, c \in G$, we have

$$(a * b) * c = a * (b * c). \quad \textbf{associativity of } *$$

$\mathscr{G}_2$: There is an element e in G such that for all $x \in G$,

$$e * x = x * e = x. \quad \textbf{identity element } e \text{ for } *$$

$\mathscr{G}_3$: Corresponding to each $a \in G$, there is an element a' in G such that

$$a * a' = a' * a = e. \quad \textbf{inverse } a' \text{ of } a$$

Ex:- $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{Q}, + \rangle$ are groups

$\langle \mathbb{Z}, \cdot \rangle$ is not a group $[2^{-1} \notin \mathbb{Z}]$

$\langle \mathbb{Q}, \cdot \rangle$ is not a group $[0^{-1}$ does not exist$]$

$\langle \mathbb{Q}^*, \cdot \rangle$ is a group $[\mathbb{Q}^* = \mathbb{Q}^- = \mathbb{Q} \setminus \{0\}]$

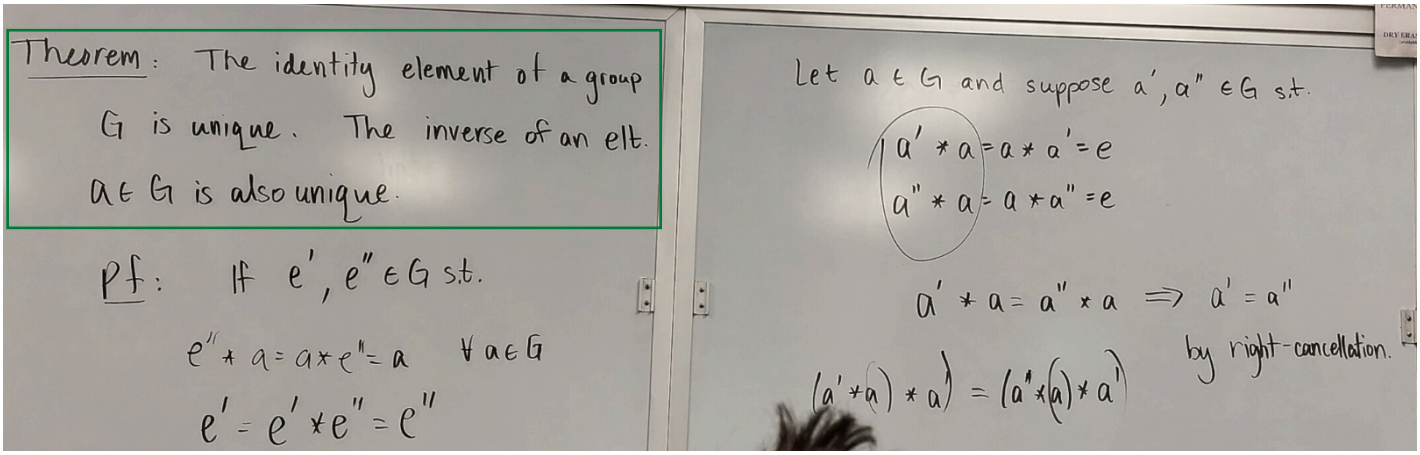
$\langle \mathbb{R}^+, \cdot \rangle$ is a group

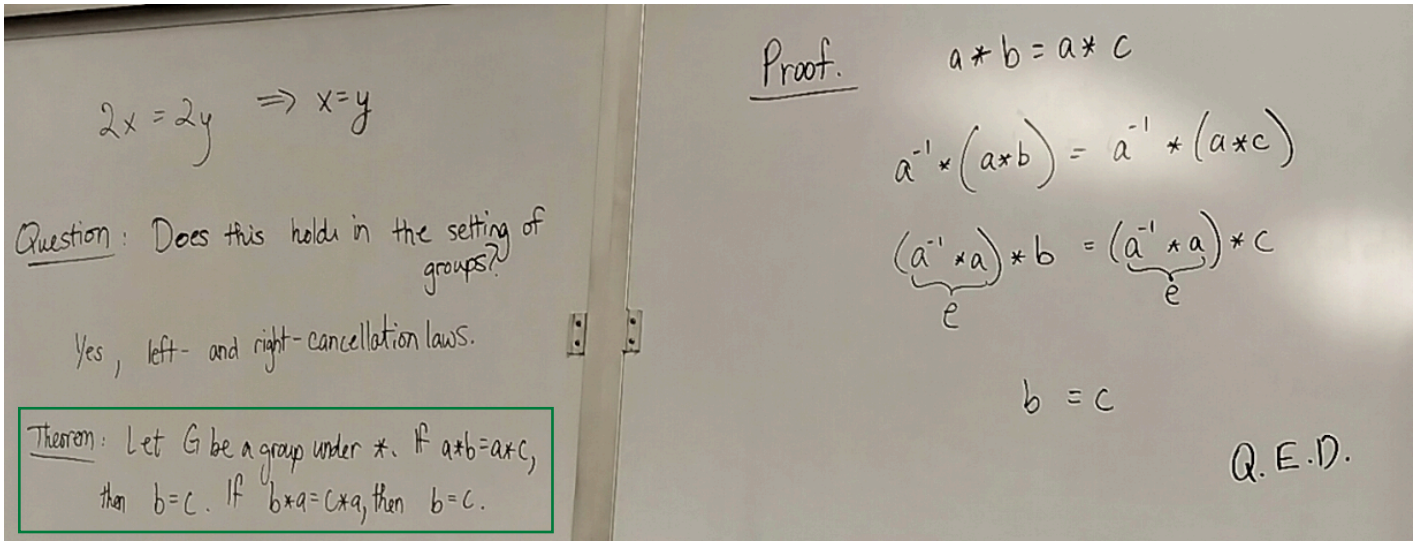
Q. $\langle M_n(\mathbb{R}), + \rangle$ is a group

$GL_n(\mathbb{R})$: general linear group of degree n

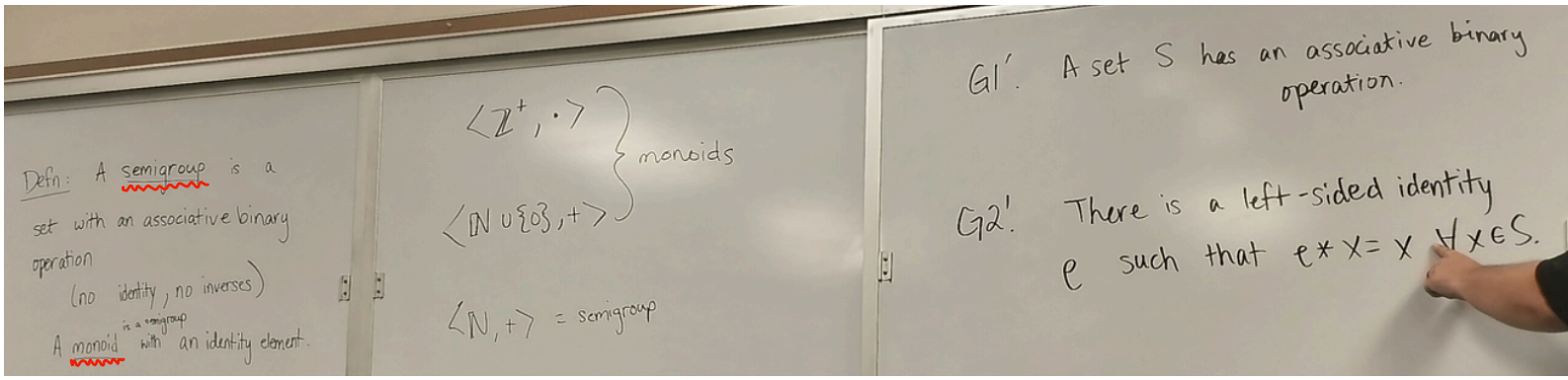
$\Downarrow \det(A) \neq 0$ — group under matrix multiplication

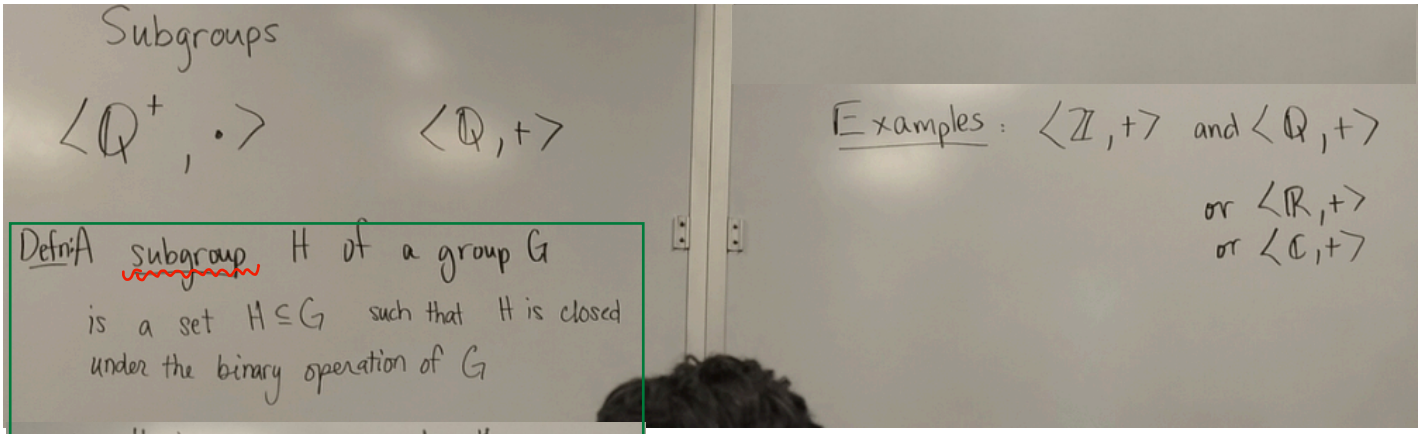
$\langle \mathbb{Q}^*, * \rangle$ such that $a * b = \frac{ab}{2}$ is a group

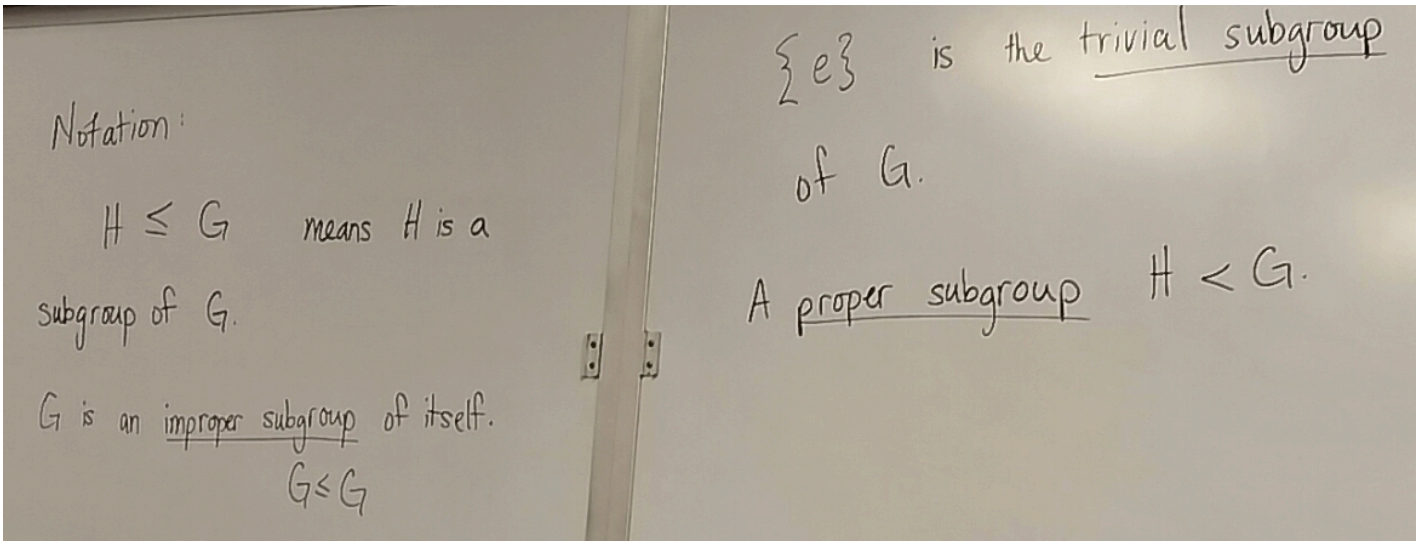




* A group G is **abelian** if its binary operation is commutative.







Ex: $n\mathbb{Z} < \mathbb{Z} \Rightarrow \mathbb{Z} > 2\mathbb{Z} > 4\mathbb{Z} > 8\mathbb{Z} > 16\mathbb{Z} > \cdots$

$U_n = \{ e^{\frac{2\pi i}{n} k} : k = 0, 1, \ldots, n-1 \}$, $\langle U_n, \cdot \rangle$

$U_8 > U_4 > U_2 > 1$

A subset H of a group G is a subgroup of G if and only if

1. H is closed under the binary operation of G,
2. the identity element e of G is in H,
3. for all $a \in H$ it is true that $a^{-1} \in H$ also.

Thm: Let G and G' be groups with binary operations $*$ and $*'$ respectively. Let $\varphi: G \to G'$ be an iso. (↑ 1-1, onto, $\varphi(g_1 * g_2) = \varphi(g_1) *' \varphi(g_2)$)

For any $H \leq G$, $\varphi(H) \leq G'$.

Proof:

(1) Let $h_1', h_2' \in \varphi(H)$.

WTS: $h_1' *' h_2' \in \varphi(H)$

$\exists\ h_1, h_2 \in H$ s.t. $\varphi(h_1) = h_1'$, $\varphi(h_2) = h_2'$

$\varphi(h_1) *' \varphi(h_2) \overset{?}{\in} \varphi(H)$

$\varphi(h_1 * h_2) \overset{?}{\in} \varphi(H)$

Since $H \leq G$, $h_1 * h_2 \in H \Rightarrow$

$\varphi(h_1 * h_2) \in \varphi(H)$.

(2) Is $e' \in \varphi(H)$?

$e \in H$ since $H \leq G$ and $\varphi(e) = e' \in \varphi(H)$

(3) Let $h' \in \varphi(H)$.

WTS: $(h')^{-1} \in \varphi(H)$.

$\exists\ h \in H$ s.t. $\varphi(h) = h'$.

Since $H \leq G$, $h^{-1} \in H$.

$e' = \varphi(e) = \varphi(h * h^{-1}) = \varphi(h) *' \varphi(h^{-1})$

$\varphi(h^{-1}) = (\varphi(h))^{-1} \in \varphi(H)$

$(h')^{-1}$

Q.E.D.

Thm: Let $a \in G$ and define $H := \{a^n : n \in \mathbb{Z}\}$.

Then $H \leq G$.

$H = \langle a \rangle$: subgroup generated by 'a'.

This is called a cyclic group.

Proof: Let $h_1, h_2 \in H$.

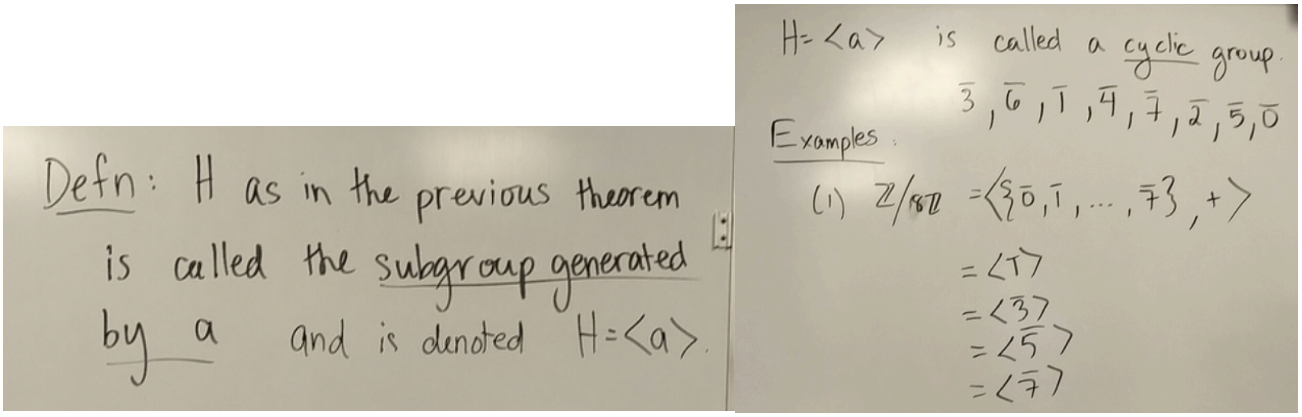
$h_1 = a^m$, $h_2 = a^k$ for some $m, k \in \mathbb{Z}$

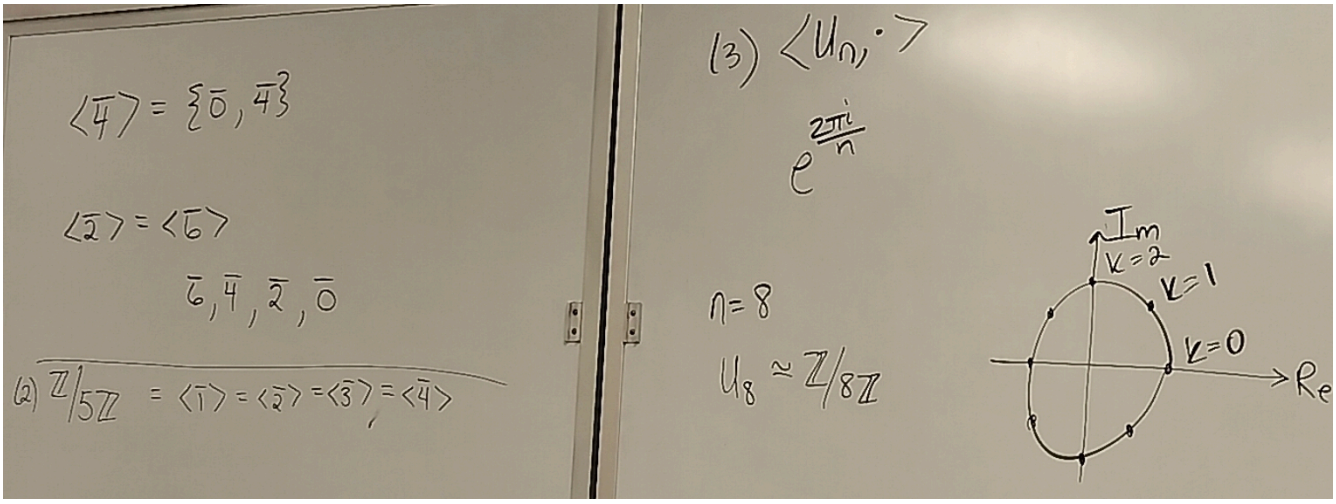
(1) $h_1 h_2 = a^m a^k = a^{m+k} \in H$

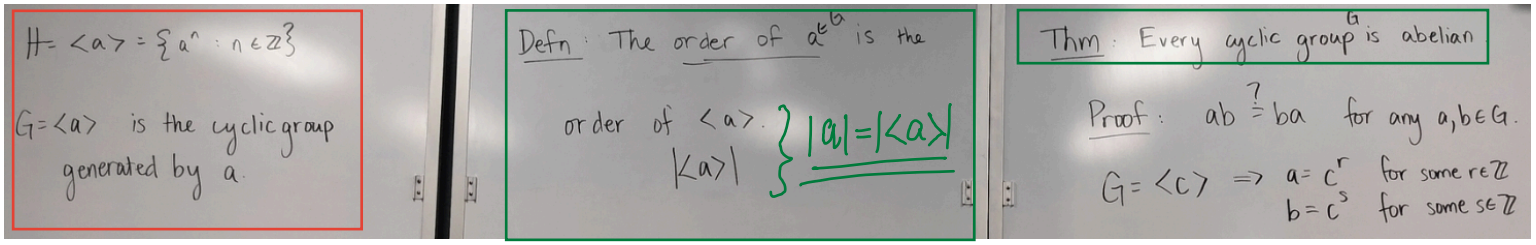
(2) $a^0 = e$ $\quad a^0 a^m = a^{0+m} = a^m$

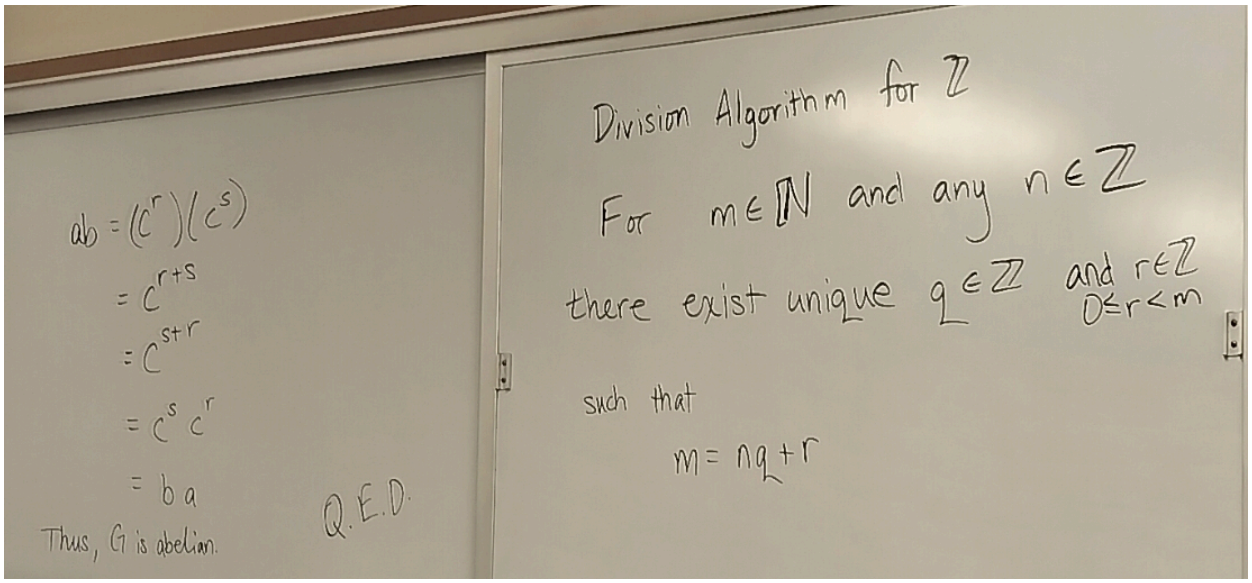
(3) For $h \in H$, $h = a^k$ $\quad h^{-1} = a^{-k}$ since $(a^k)(a^{-k}) = a^0 = e$

$\therefore$ H is a subgroup of G.



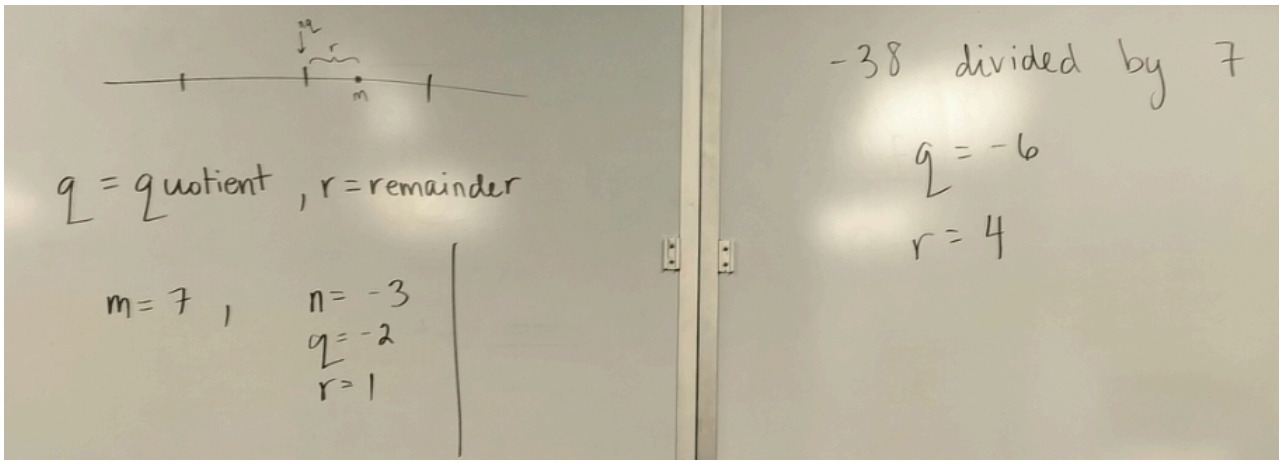






Division Algorithm for $\mathbb{Z}$ If m is a positive integer and n is any integer, then there exist unique integers q and r such that

$$n = mq + r \qquad \text{and} \qquad 0 \leq r < m.$$



Theorem A subgroup of a cyclic group is cyclic.

Proof Let G be a cyclic group generated by a and let H be a subgroup of G. If $H = \{e\}$, then $H = \langle e \rangle$ is cyclic. If $H \neq \{e\}$, then $a^n \in H$ for some $n \in \mathbb{Z}^+$. Let m be the smallest integer in $\mathbb{Z}^+$ such that $a^m \in H$.

We claim that $c = a^m$ generates H; that is,

$$H = \langle a^m \rangle = \langle c \rangle.$$

We must show that every $b \in H$ is a power of c. Since $b \in H$ and $H \leq G$, we have $b = a^n$ for some n. Find q and r such that

$$n = mq + r \qquad \text{for} \qquad 0 \leq r < m$$

in accord with the division algorithm. Then

$$a^n = a^{mq+r} = (a^m)^q a^r,$$

so

$$a^r = (a^m)^{-q} a^n.$$

Now since $a^n \in H$, $a^m \in H$, and H is a group, both $(a^m)^{-q}$ and a^n are in H. Thus

$$(a^m)^{-q} a^n \in H; \qquad \text{that is,} \qquad a^r \in H.$$

Since m was the smallest positive integer such that $a^m \in H$ and $0 \leq r < m$, we must have $r = 0$. Thus $n = qm$ and

$$b = a^n = (a^m)^q = c^q,$$

so b is a power of c. ◆

As noted in Examples 5.21 and 5.22, $\mathbb{Z}$ under addition is cyclic and for a positive integer n, the set $n\mathbb{Z}$ of all multiples of n is a subgroup of $\mathbb{Z}$ under addition, the cyclic subgroup generated by n. Theorem 6.6 shows that these cyclic subgroups are the only subgroups of $\mathbb{Z}$ under addition. We state this as a corollary.

Thm: Let G be a cyclic group with n elements and generated by a. Let $b \in G$ with $b = a^s$. Then b generates a subgroup with $\frac{n}{d}$ elements where $d = (n, s)$.

Let $G = \langle a \rangle$ & $|G| = n$,

$\langle b \rangle = \langle a^s \rangle \leq G$ with

$|\langle a^s \rangle| = \frac{n}{\gcd(n,s)}$

Proof: Clearly $\langle b \rangle$ is a subgroup of G. $b = a^s$, let m be the smallest integer such that $b^m = e$.

$(a^s)^m = a^{sm} = e$

The only way $a^k = e$ is if $n \mid k \Rightarrow n \mid sm$.

n divides k.

Let $d = (s, n)$. There exist $u, v \in \mathbb{Z}$

$d = us + vn$

$1 = u\left(\frac{s}{d}\right) + v\left(\frac{n}{d}\right)$ } $\gcd\left(\frac{s}{d}, \frac{n}{d}\right) = 1$

$\frac{sm}{n} = \frac{\left(\frac{s}{d}\right)m}{\left(\frac{n}{d}\right)} \Rightarrow$ we must have $\frac{n}{d} \mid m$ and it follows m is at least $\frac{n}{d} \Rightarrow m = \frac{n}{d}$.

Thus, $|\langle b \rangle| = \frac{n}{d}$.

Q.E.D.

Section 7 : Generating Sets and Cayley Digraphs

Generating Sets $= \langle a, b \rangle$

$\approx \{ a^m b^n : m, n \in \mathbb{Z} \}$

need not have to be commutative

ab abab ababab

Klein-4 group : $\{(\bar{0},\bar{0}), (\bar{1},\bar{0}), (\bar{0},\bar{1}), (\bar{1},\bar{1})\}$ (a, b, c)

with $\frac{1}{2}$

$\{ a, b, c, e : a^2 = b^2 = c^2 = e, ab = c \}$

$\langle a, b \rangle = \langle a, c \rangle = \langle b, c \rangle$

$\langle a^s \rangle = \langle a^t \rangle$ if and only if

$(s, n) = (t, n) \Rightarrow \gcd(s, n) = \gcd(t, n)$

$\mathbb{Z}/12\mathbb{Z}$,

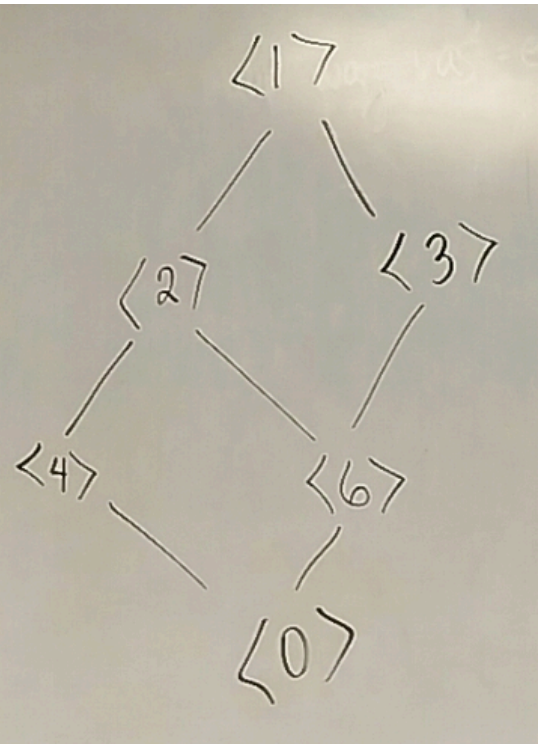
$\langle 6 \rangle$

$\langle 4 \rangle = \langle 8 \rangle$

$\langle 3 \rangle = \langle 9 \rangle$

$\langle 2 \rangle = \langle 10 \rangle$

$\langle 1 \rangle = \langle 7 \rangle = \langle 11 \rangle = \langle 5 \rangle$



$\mathbb{Z}_{18} = \mathbb{Z}/18\mathbb{Z} = \{0,1,2,\ldots,17\}$

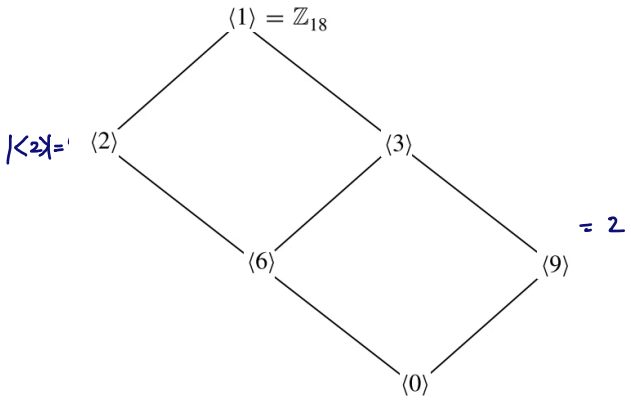
Lagrange's theorem:

$|\langle g\rangle| \mid |G| \Rightarrow$ divisors of $18 = \{1,2,3,6,9,18\}$

Subgroup of order $1 = \langle 0\rangle$, " order $2 = \langle \frac{18}{2}\rangle = \langle 9\rangle = \{0,9\}$

" order $3 = \langle \frac{18}{3}\rangle = \langle 6\rangle = \{0,6,12\}$

$|H_1| \mid |H_2| \Rightarrow H_1 \leq H_2$

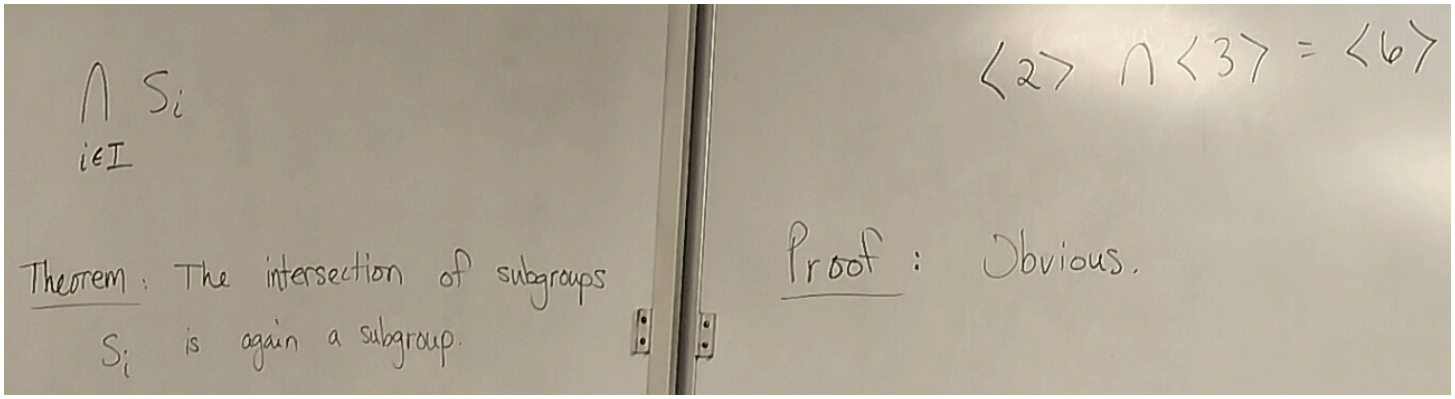


6.18 Figure Subgroup diagram for $\mathbb{Z}_{18}$.

$\langle 0\rangle \leq \langle 9\rangle \leq \langle 3\rangle \leq \langle 1\rangle$

$\langle 0\rangle \leq \langle 6\rangle \leq \langle 3\rangle \leq \langle 1\rangle$

$\langle 0\rangle \leq \langle 6\rangle \leq \langle 2\rangle \leq \langle 1\rangle$

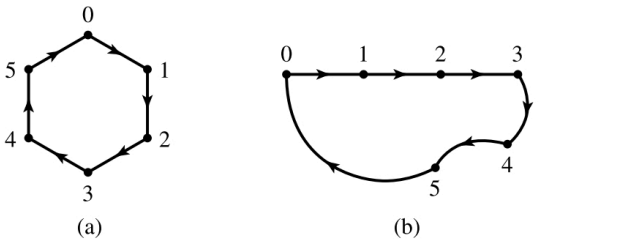


Cayley Digraphs

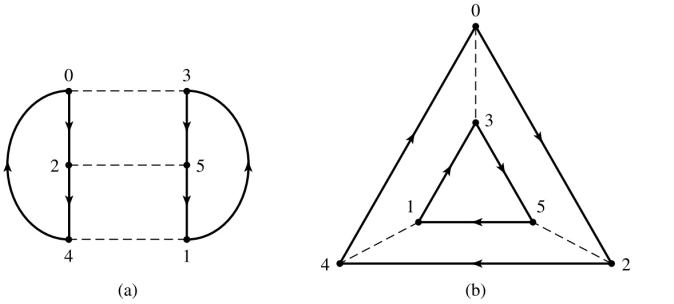
Intuitively, a **digraph** consists of a finite number of points, called **vertices** of the digraph, and some **arcs** (each with a direction denoted by an arrowhead) joining vertices. In a digraph for a group G using a generating set S we have one vertex, represented by a dot, for each element of G. Each generator in S is denoted by one type of arc. We could use different colors for different arc types in pencil and paperwork. Since different colors are not available in our text, we use different style arcs, like solid, dashed, and dotted, to denote different generators. Thus if $S = \{a, b, c\}$ we might denote

a by ——➤——, b by - - -➤- - -, and c by ·····➤·····.

With this notation, an occurrence of x•——➤——•y in a Cayley digraph means that $xa = y$. That is, traveling an arc in the direction of the arrow indicates that multiplication of the group element at the start of the arc *on the right* by the generator corresponding to that type of arc yields the group element at the end of the arc. Of course, since we are in a group, we know immediately that $ya^{-1} = x$. Thus traveling an arc in the direction opposite to the arrow corresponds to multiplication on the right by the inverse of the corresponding generator. If a generator in S is its own inverse, it is customary to denote this by omitting the arrowhead from the arc, rather than using a double arrow. For example, if $b^2 = e$, we might denote b by ————————.

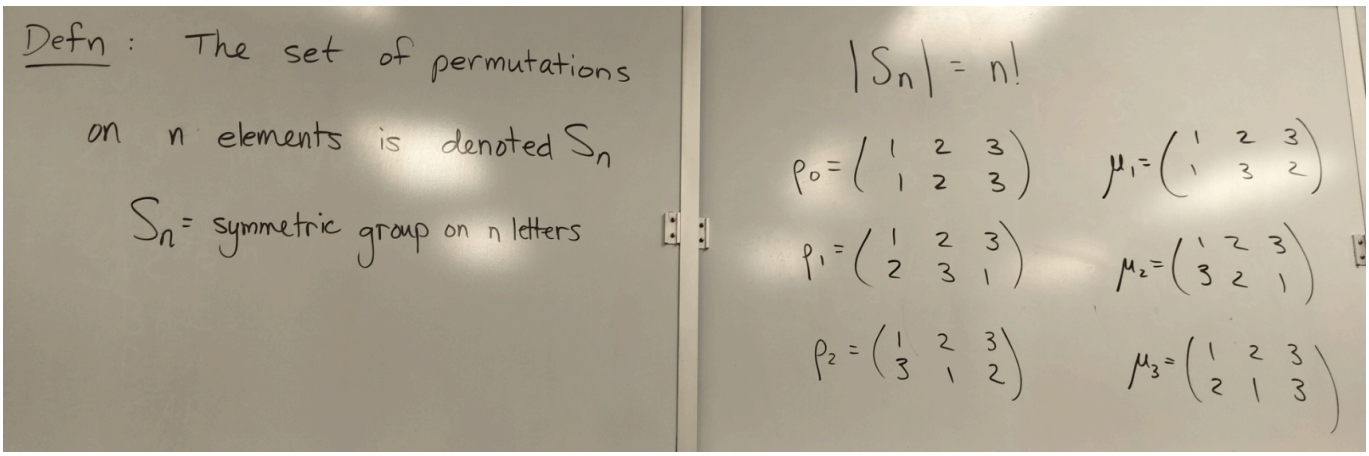


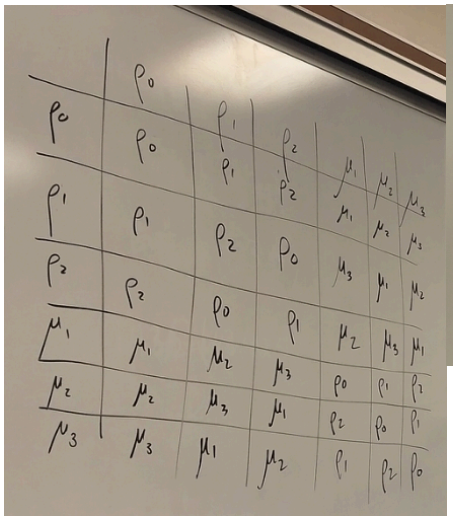
7.8 Figure Two digraphs for $\mathbb{Z}_6$ with $S = \{1\}$ using ——➤——$_1$.

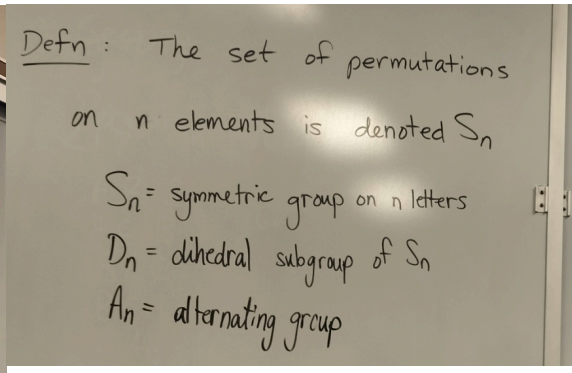


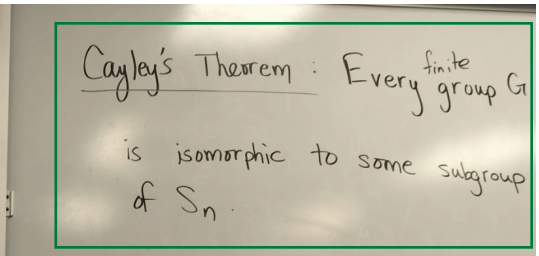
7.9 Figure Two digraphs for $\mathbb{Z}_6$ with $S = \{2, 3\}$ using ——➤——$_2$ and ————————$_3$.

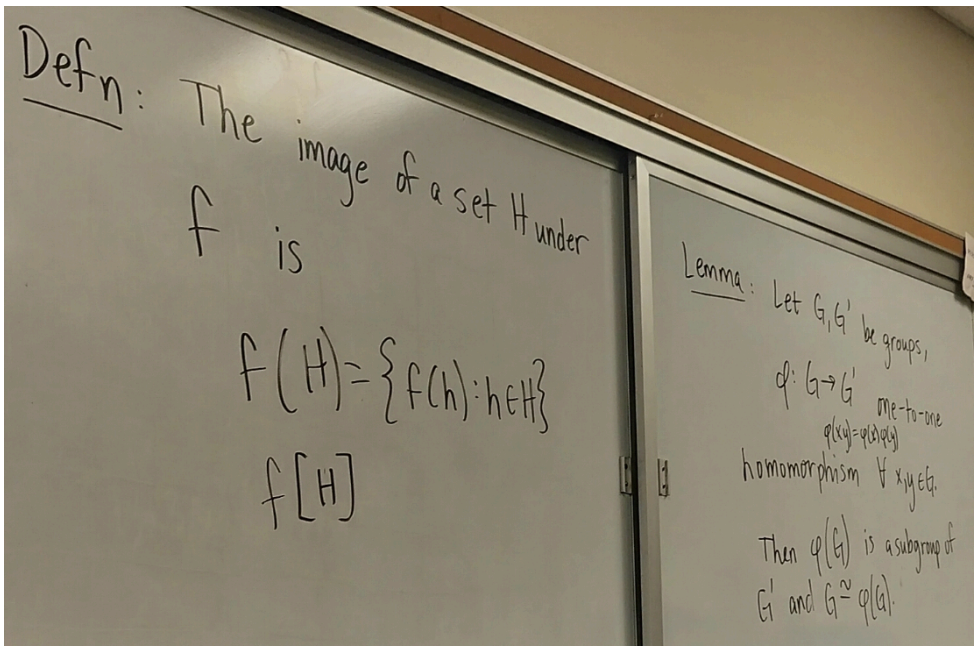
$\mathbb{Z}_n / 6\mathbb{Z}$

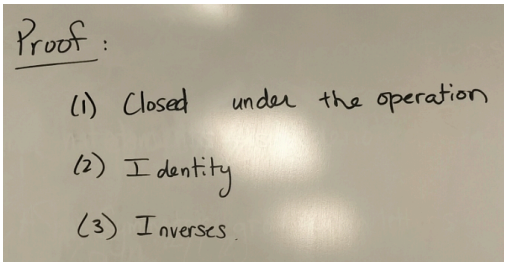












8.14 Definition Let $f : A \to B$ be a function and let H be a subset of A. The **image of H under f** is $\{f(h) \mid h \in H\}$ and is denoted by $f[H]$. ■

8.15 Lemma Let G and G' be groups and let $\phi : G \to G'$ be a one-to-one function such that $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$. Then $\phi[G]$ is a subgroup of G' and ϕ provides an isomorphism of G with $\phi[G]$.

(Cayley's Theorem) Every group is isomorphic to a group of permutations.

The orbit of an element 'a' under a permutation σ is the set of all elements that 'a' can be mapped to by repeated applications of σ.

Let A be a set and let $\sigma \in S_A$. For a fixed $a \in A$, the set $\mathcal{O}_{a,\sigma} = \{\sigma^n(a) : n \in \mathbb{Z}\}$ is the orbit of 'a' under σ.

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}$$

$\tau(1) = 2, \tau(2) = 4, \tau(4) = 3, \tau(3) = 1$

$\therefore$ The orbit of 1 under the permutation τ is,

$$\mathcal{O}_{1,\tau} = \{1, 2, 3, 4\}$$

element a in a group G has order $r > 0$ if $a^r = e$ and no smaller positive power of a is the identity.

A permutation $\sigma \in S_n$ is a **cycle** if it has at most one orbit containing more than one element. The **length** of a cycle is the number of elements in its largest orbit.

S_8 is the symmetric group on the set $\{1,2,3,4,5,6,7,8\}$, which consists of all possible permutations of the 8 elements in the set.

(a) What is the order of the cycle (1457)? What about the order of (57326)?

Ans: $(1\,4\,5\,7) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 3 & 5 & 7 & 6 & 1 & 8 \end{pmatrix}$

order of $(1\,4\,5\,7) = 4$.

because if we apply the permutation 4 times, the elements will return to their original positions.

$(5\,7\,3\,2\,6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 6 & 2 & 4 & 7 & 5 & 3 & 8 \end{pmatrix}$

order of $(5\,7\,3\,2\,6) = 5$.

(b) State a theorem suggest by (a). You do not need to prove it.

Ans: Theorem – The order of a cycle in a symmetric group is equal to the # of elements in the cycle.

(c) What is the order of $\sigma = (45)(237)$? of $\tau = (14)(3578)$?

Ans: The 2-cycle (45) returns to the identity after 2 applications, and the 3-cycle (237) returns to the identity after 3 applications. Therefore, the order of $\sigma = (45)(237)$ is the smallest # of applications after which both cycles have returned to the identity.

∴ The order of $\sigma = (45)(237)$ is $LCM(2,3) = 6$.

Similarly,

the order of $(14) = 2$

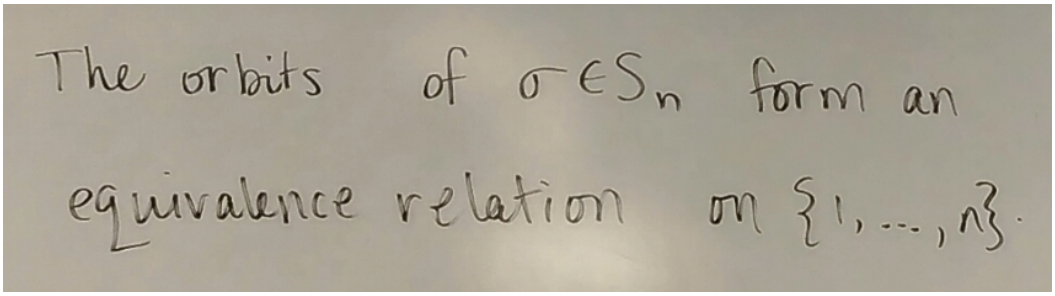
the order of $(3578) = 4$

∴ The order of $\tau = (14)(3578) = LCM(2,4) = 4$.

(d) State a theorem suggest by (c). You do not need to prove it.

Ans:

Theorem – The order of a permutation that is the product of disjoint cycles is the least common multiple (LCM) of the orders of the individual cycles.



Each permutation σ of a set A determines a natural partition of A into cells with the property that $a, b \in A$ are in the same cell if and only if $b = \sigma^n(a)$ for some $n \in \mathbb{Z}$. We establish this partition using an appropriate equivalence relation:

$$\text{For } a, b \in A, \text{ let } a \sim b \text{ if and only if } b = \sigma^n(a) \text{ for some } n \in \mathbb{Z}. \qquad \textbf{(1)}$$

We now check that $\sim$ defined by Condition (1) is indeed an equivalence relation.

Reflexive Clearly $a \sim a$ since $a = \iota(a) = \sigma^0(a)$.

Symmetric If $a \sim b$, then $b = \sigma^n(a)$ for some $n \in \mathbb{Z}$. But then $a = \sigma^{-n}(b)$ and $-n \in \mathbb{Z}$, so $b \sim a$.

Transitive Suppose $a \sim b$ and $b \sim c$, then $b = \sigma^n(a)$ and $c = \sigma^m(b)$ for some $n, m \in \mathbb{Z}$. Substituting, we find that $c = \sigma^m(\sigma^n(a)) = \sigma^{n+m}(a)$, so $a \sim c$.

Let σ be a permutation of a set A. The equivalence classes in A determined by the equivalence relation (1) are the **orbits of** σ. ■

Since the identity permutation ι of A leaves each element of A fixed, the orbits of ι are the one-element subsets of A. ▲

Theorem Every permutation σ of a finite set is a product of disjoint cycles.

Proof Let $B_1, B_2, \cdots, B_r$ be the orbits of σ, and let μ_i be the cycle defined by

$$\mu_i(x) = \begin{cases} \sigma(x) & \text{for } x \in B_i \\ x & \text{otherwise.} \end{cases}$$

Clearly $\sigma = \mu_1 \mu_2 \cdots \mu_r$. Since the equivalence-class orbits $B_1, B_2, \cdots, B$, being distinct equivalence classes, are disjoint, the cycles $\mu_1, \mu_2, \cdots, \mu_r$ are disjoint also. ◆

While permutation multiplication in general is not commutative, it is readily seen that *multiplication of disjoint cycles is commutative*. Since the orbits of a permutation are unique, the representation of a permutation as a product of disjoint cycles, none of which is the identity permutation, is unique up to the order of the factors.

9.9 Example Consider the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix}.$$

Let us write it as a product of disjoint cycles. First, 1 is moved to 6 and then 6 to 1, giving the cycle (1, 6). Then 2 is moved to 5, which is moved to 3, which is moved to 2, or (2, 5, 3). This takes care of all elements but 4, which is left fixed. Thus

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix} = (1, 6)(2, 5, 3).$$

Multiplication of *disjoint* cycles is commutative, so the order of the factors (1, 6) and (2, 5, 3) is not important. ▲

9.10 Example Consider the cycles (1,4,5,6) and (2,1,5) in S_6. Multiplying, we find that

$$(1, 4, 5, 6)(2, 1, 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix}$$

and

$$(2, 1, 5)(1, 4, 5, 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix}.$$

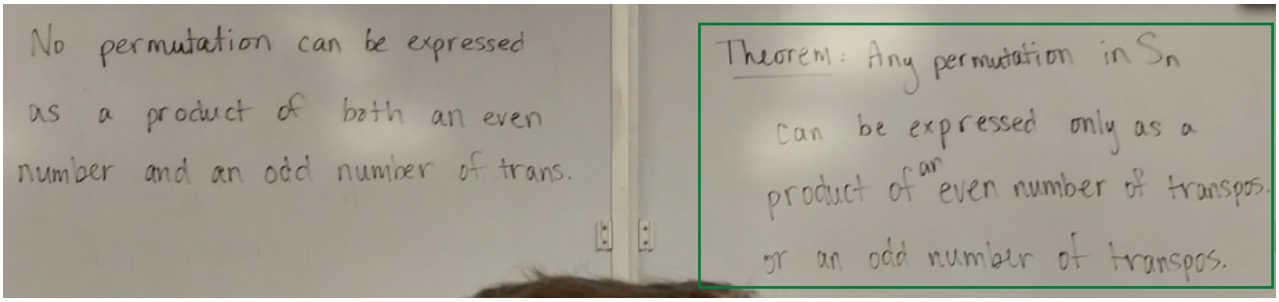
Neither of these permutations is a cycle.

A cycle of length 2 is a **transposition**. ■

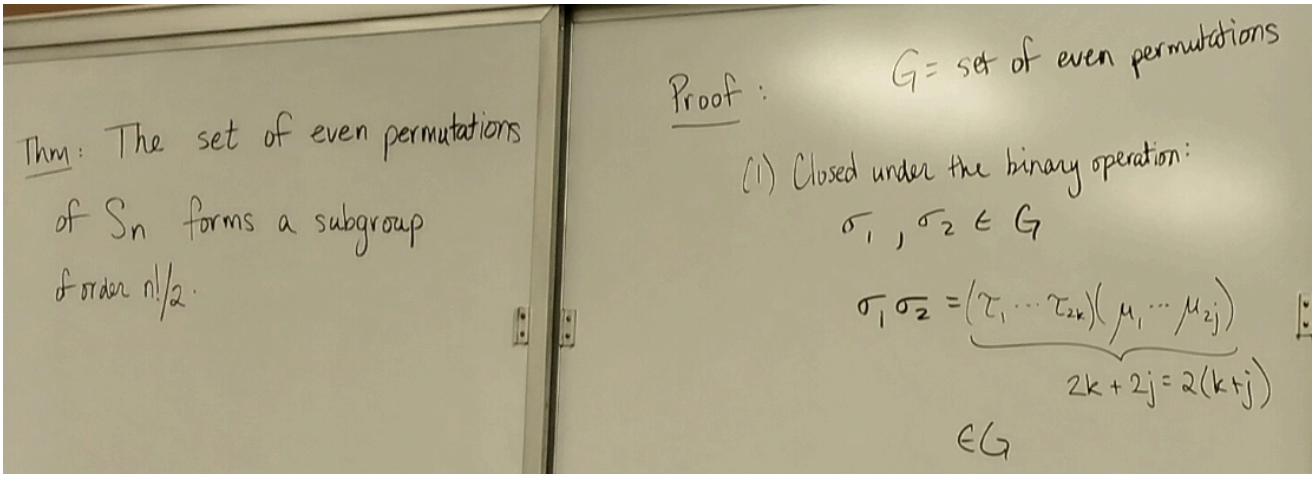
Thus a transposition leaves all elements but two fixed, and maps each of these onto the other. A computation shows that

$$(a_1, a_2, \cdots, a_n) = (a_1, a_n)(a_1, a_{n-1}) \cdots (a_1, a_3)(a_1, a_2).$$

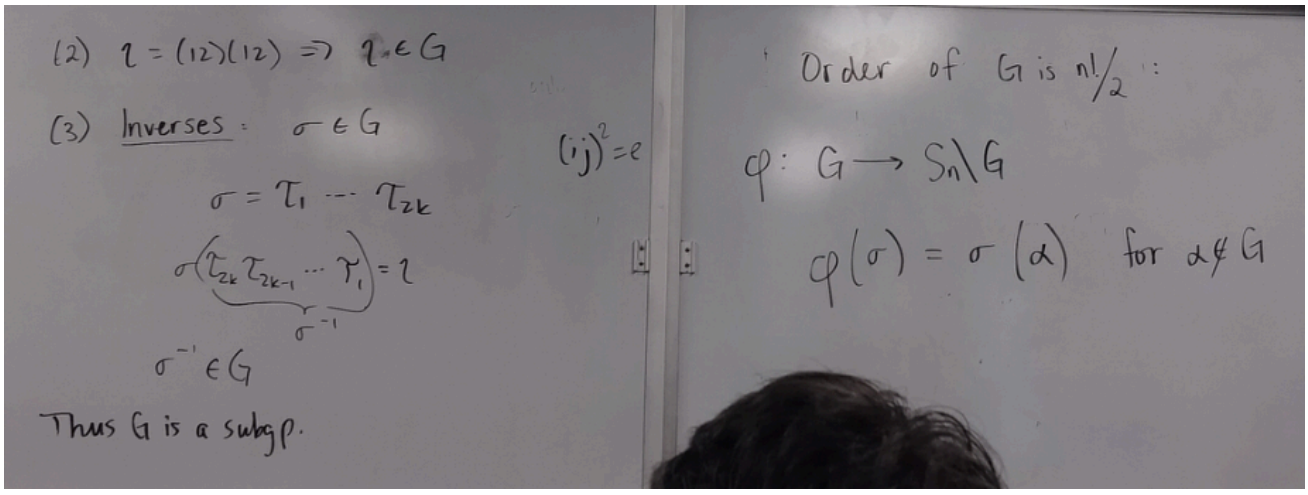
Therefore any cycle is a product of transpositions.



Proof 1 (From linear algebra) We remarked in Section 8 that $S_A \simeq S_B$ if A and B have the same cardinality. We work with permutations of the n rows of the $n \times n$ identity matrix I_n, rather than of the numbers $1, 2, \ldots, n$. The identity matrix has determinant 1. Interchanging any two rows of a square matrix changes the sign of the determinant. Let C be a matrix obtained by a permutation σ of the rows of I_n. If C could be obtained from I_n by both an even number and an odd number of transpositions of rows, its determinant would have to be both 1 and -1, which is impossible. Thus σ cannot be expressed both as a product of an even number and an odd number of transpositions.



* The subgroup of S_n consisting of the even permutations of n letters is the alternating group A_n on n letters.



Theorem Let H be a subgroup of G. Let the relation $\sim_L$ be defined on G by

$$a \sim_L b \qquad \text{if and only if} \qquad a^{-1}b \in H.$$

Let $\sim_R$ be defined by

$$a \sim_R b \qquad \text{if and only if} \qquad ab^{-1} \in H.$$

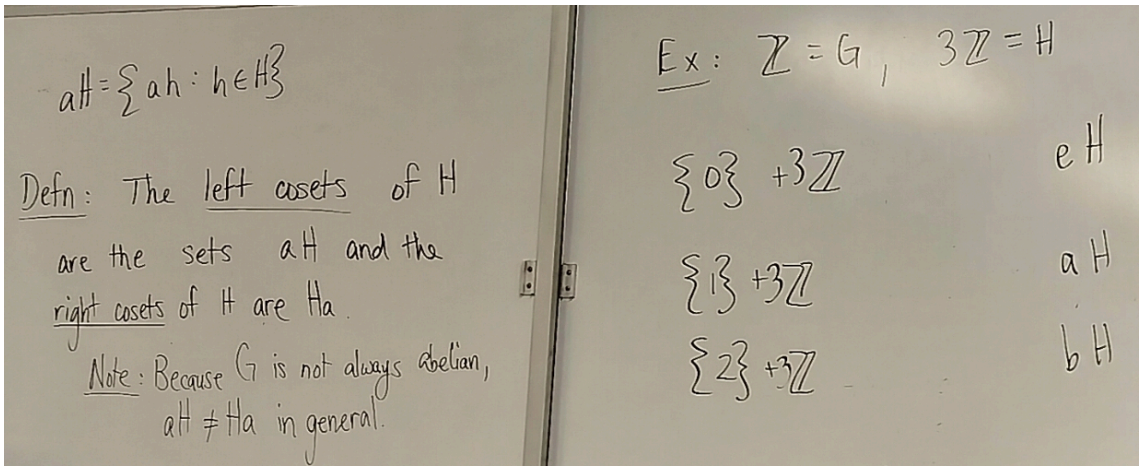
Then $\sim_L$ and $\sim_R$ are both equivalence relations on G.

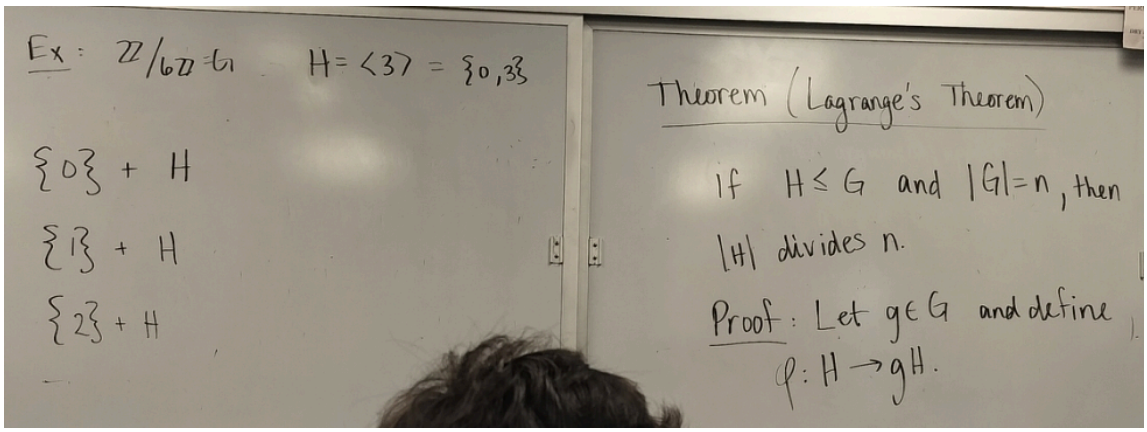
Proof We show that $\sim_L$ is an equivalence relation, and leave the proof for $\sim_R$ to Exercise 26. When reading the proof, notice how we must constantly make use of the fact that H is a *subgroup* of G.

Reflexive Let $a \in G$. Then $a^{-1}a = e$ and $e \in H$ since H is a subgroup. Thus $a \sim_L a$.

Symmetric Suppose $a \sim_L b$. Then $a^{-1}b \in H$. Since H is a subgroup, $(a^{-1}b)^{-1}$ is in H and $(a^{-1}b)^{-1} = b^{-1}a$, so $b^{-1}a$ is in H and $b \sim_L a$.

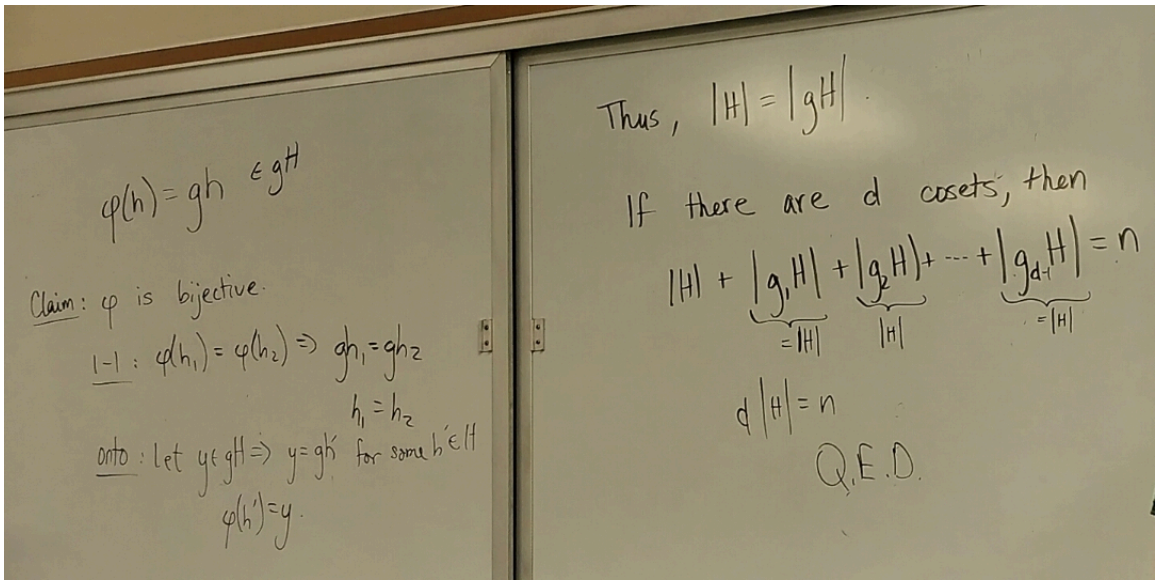
Transitive Let $a \sim_L b$ and $b \sim_L c$. Then $a^{-1}b \in H$ and $b^{-1}c \in H$. Since H is a subgroup, $(a^{-1}b)(b^{-1}c) = a^{-1}c$ is in H, so $a \sim_L c$. ◆

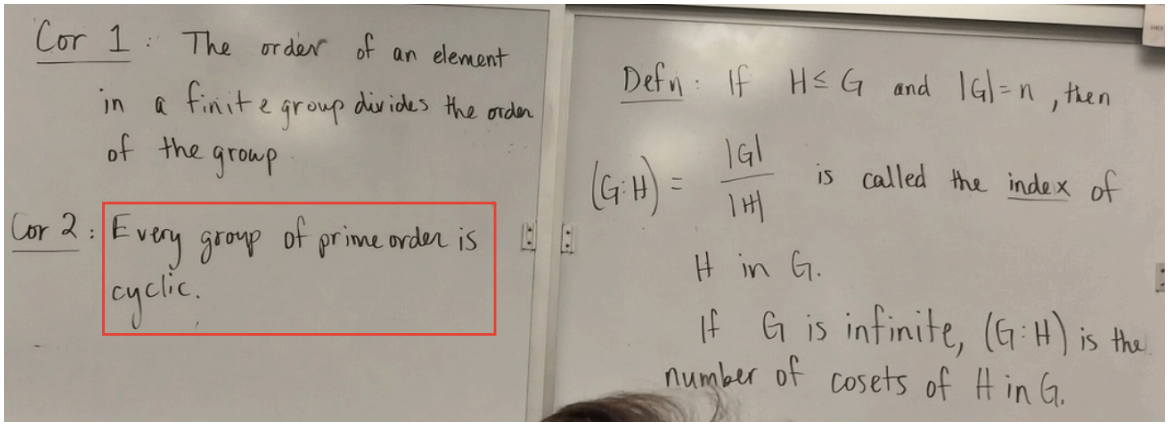




$|G| = (G:H)|H|$

$(G:H)$: index of H in G
– # of distinct cosets of H in G.




Cor 1: The order of an element in a finite group divides the order of the group.
Cor 2: Every group of prime order is cyclic.
Defn: If $H \leq G$ and $|G| = n$, then
$(G:H) = \frac{|G|}{|H|}$ is called the index of H in G.
If G is infinite, $(G:H)$ is the number of cosets of H in G.