Modern Algebra and Number Systems
Lesson 10
Subgroups

This lesson has two parts. Part 1 is required for all students. Part 2 is only required for MAT615 students.

Part I

Review groups from before Exam 1. You may also wish to review inverses of matrices which explains how to find inverses of matrices.

Watch Playlist 314F20-10-Part1 and do HW1-5:
I apologize for the audio going in and out but you can hear it all if you turn up the volume. I think the cord for my microphone is either broken or was going in an out of the socket. Note that everything of importance is written down so you can probably watch it silently if that is easier for you.

Lesson 10

SUBGROUPS

Review $(G,*)$ is a group if it's

- a binary operation $a,b\in G \Rightarrow a*b\in G$
- associative $\forall a,b,c\in G$ $a*(b*c)=(a*b)*c$
- has an identity e: $e*a=a*e=a$ $\forall a\in G$
- each element $a\in G$ has an inverse $a^{-1}\in G$ s.t. $a*a^{-1}=a^{-1}*a=e$.

DEFINITION A subset H of a group $(G,*)$ is called a **subgroup** of G if the elements of H form a group under $*$.

$2\mathbb{Z}$ = even integers

$(2\mathbb{Z},+)$ is a subgroup of $(\mathbb{Z},+)$

$\left\{\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix} : a,b,c\in\mathbb{R}\right\}$ is a subgroup of $GL(3,\mathbb{R})$ with matrix mult.

THEOREM 5.1 Let H be a nonempty subset of a group G. Then H is a subgroup of G if and only if the following two conditions are satisfied:

i) for all $a,b\in H$, $ab\in H$, (closed under $*$)

ii) for all $a\in H$, $a^{-1}\in H$. (closed under inverses)

Proof (on right)

$\boxed{\text{HW1}}$ Use Thm 5.1 to prove $\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix} \middle|\ ad-bc=1\right\}$ is a subgroup of $GL(2,\mathbb{R})$

Example: $(2\mathbb{Z},+)$ is a subgroup of $(\mathbb{Z},+)$

$(2\mathbb{Z},+)$ is a group because

- binary operation ✓
  add even numbers
  Given any $a,b\in 2\mathbb{Z}=\{2j : j\in\mathbb{Z}\}$
  we can write $a=2n$ $b=2m$
  where $n,m\in\mathbb{Z}$
  by the defn of $2\mathbb{Z}$
  $a+b=2n+2m=2(n+m)$ by factoring
  $\in 2\mathbb{Z}$ because $n+m\in\mathbb{Z}$
- assoc is true because $+$ is assoc ✓
  for all integers.
- identity 0 $\quad 0+a=a=a+0$ for any $a\in 2\mathbb{Z}$ ✓
- inverses: if $a\in 2\mathbb{Z}$, $a=2n$ for some $n\in\mathbb{Z}$
  $-a=-2n=2(-n)\in 2\mathbb{Z}$
  because $-n\in\mathbb{Z}$ when $n\in\mathbb{Z}$
  $a+(-a)=0=(-a)+a$ ✓

Thus $2\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

Example: Show $\left\{\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix} \;\middle|\; a,b,c\in\mathbb{R}\right\} = H$

is a subgroup of $GL(3,\mathbb{R})$.

Recall $GL(3,\mathbb{R})$ are invertible matrices and

$\begin{pmatrix}\boxed{1}&a&b\\0&\boxed{1}&c\\0&0&\boxed{1}\end{pmatrix}$ is invertible because it has 3 leaders.

So H is a subset of $G=GL(3,\mathbb{R})$

To prove H is a subgroup

Show it is a group.

- binary operation

$$\begin{pmatrix}1&a_1&b_1\\0&1&c_1\\0&0&1\end{pmatrix}\times\begin{pmatrix}1&a_2&b_2\\0&1&c_2\\0&0&1\end{pmatrix} =$$

$$=\begin{pmatrix}1&a_2+a_1&b_2+c_2a_1+b_1\\0&1&c_2+c_1\\0&0&1\end{pmatrix}\in H$$

because 0 below diag, 1 on diag, reals above

- associative because matrix mult is assoc

- Identity we know $I=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$ has $M\times I = M = I\times M \;\forall M\in G$

Check $I\in H$: Yes: $a=b=c=0$ ✓

- Inverses $\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}^{-1}$ use row red ✓

$$\left(\begin{array}{ccc|ccc}1&a&b&1&0&0\\0&1&c&0&1&0\\0&0&1&0&0&1\end{array}\right)\xrightarrow[\rho_2-c\rho_3]{}\left(\begin{array}{ccc|ccc}1&a&b&1&0&0\\0&1&0&0&1&-c\\0&0&1&0&0&1\end{array}\right)\xrightarrow[\rho_1-b\rho_3]{}$$

$$\left(\begin{array}{ccc|ccc}1&a&0&1&0&-b\\0&1&0&0&1&-c\\0&0&1&0&0&1\end{array}\right)\xrightarrow[\rho_1-a\rho_2]{}\left(\begin{array}{ccc|ccc}1&0&0&1&-a&-b+ac\\0&1&0&0&1&-c\\0&0&1&0&0&1\end{array}\right)$$

Inverse is $\begin{pmatrix}1&-a&-b+ac\\0&1&-c\\0&0&1\end{pmatrix}\in H$ zeroes below diag, 1 on diag, real above

$$\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\begin{pmatrix}1&-a&-b+ac\\0&1&-c\\0&0&1\end{pmatrix}$$

$$=\begin{pmatrix}1&0&\cancel{-b+ac-ac+b}\;0\\0&1&0\\0&0&1\end{pmatrix}=I$$

$$\begin{pmatrix}1&-a&-b+ac\\0&1&-c\\0&0&1\end{pmatrix}\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}=\sim\sim=I$$

3:12 AM Sun Sep 27

Abstract_Algebra_1-5

Modern Algebra & Number Systems | Abstract_Algebra_1-5

Lesson 10

SECTION 5

SUBGROUPS

Review $(G,*)$ is a group if it is
- a binary operation $a,b\in G \Rightarrow a*b\in G$
- associative $\forall a,b,c\in G$ $a*(b*c)=(a*b)*c$
- has an identity e $e*a=a*e=a$ $\forall a\in G$
- each element $a\in G$ has an inverse $a^{-1}\in G$ s.t. $a*a^{-1}=a^{-1}*a=e$

DEFINITION A subset H of a group $(G,*)$ is called a **subgroup** of G if the elements of H form a group under $*$.

$2\mathbb{Z}$ = even integers
$(2\mathbb{Z},+)$ is a subgroup of $(\mathbb{Z},+)$

$\left\{\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix} : a,b,c\in\mathbb{R}\right\}$ is a subgroup of $GL(3,\mathbb{R})$ with matrix mult.

THEOREM 5.1 Let H be a nonempty subset of a group G. Then H is a subgroup of G if and only if the following two conditions are satisfied:

i) for all $a,b\in H$, $ab\in H$, closed under $*$
ii) for all $a\in H$, $a^{-1}\in H$. closed under inverses

Proof (on right)

HW1 Use Thm 5.1 to prove $\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix} \middle| ad-bc=1\right\}$ is a subgroup of $GL(2,\mathbb{R})$

Modern Algebra & Number Systems

Linear Algebra | Modern Algebra & Number Systems

35%

Proof of Thm 5.1:

Given:
Closed under $*$: $\forall a,b\in H$ $a*b\in H$
Closed under inverses: $\forall a\in H$ $\exists a^{-1}\in H$

Show binary, assoc, identity and inverses.

Proof:
1. binary — 1. by closed under $*$
2. assoc — 2. $*$ is assoc on G and $H\subset G$
3. inverses — 3. closed under inverses
4. identity can be found take $a\in H$ and set $e=a*a^{-1}\in H$ — 4. $a^{-1}\in H$ by closed under inverse and $a*a^{-1}\in H$ by closed under $*$

QED

Key Examples of Subgroups

$(\mathbb{C}, \times)$ not a group

$(\mathbb{C}\setminus\{0\}, \times)$ is a group

$i = 0 + 1i \in \mathbb{C}$

$\langle i \rangle = \{1, i, i^2, i^3, \ldots, i^{-1}, i^{-2}, \ldots\}$

$i^2 = -1$
$i^3 = -1 \cdot i = -i$
$i^4 = i^2 \cdot i^2 = (-1)(-1) = +1$

$i \cdot i^3 = 1$
$i^3 = i^{-1}$

$i^0 \quad i^1 \quad i^2 \quad i^{-1} = i^3$

$\langle i \rangle = \{1, i, -1, -i\}$ ← unit $\mathbb{C}$ numbers

	1	i	-1	-i
1				
i				
-1				
-i				

← can make the table.

$(\mathbb{R}\setminus\{0\}, \times) \subset (\mathbb{C}\setminus\{0\}, \times)$

↑ subset a group

So this is a subgroup.

$GL(2,\mathbb{C}) = \left\{ \begin{pmatrix} a_1+a_2 i & b_1+b_2 i \\ c_1+c_2 i & d_1+d_2 i \end{pmatrix} : \text{invertible} \right\}$

Quaternion Group

$Q_8 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} \right\}$

$Q_8 = \{I, J, K, L, -I, -J, -K, -L\}$

↑ A subgroup. See book for proof

9. Let $G = GL(2, \mathbb{C})$, the general linear group of degree two over the complex numbers. This is the set of all invertible matrices

$$\begin{pmatrix} a_1 + a_2 i & b_1 + b_2 i \\ c_1 + c_2 i & d_1 + d_2 i \end{pmatrix},$$

where the a's, b's, c's, and d's are real numbers and $i^2 = -1$, under matrix multiplication. [All you need to know about multiplying complex numbers at this point is that

$$(a+bi)(c+di) = (ac - bd) + (bc + ad)i.$$

That is, you just multiply it out and replace i^2 by -1.]

We are going to consider a subgroup of G that is of order 8, called th **group of unit quaternions**.

Let

$$J = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad K = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \text{and} \quad L = JK = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Let $Q_8 = \{I, -I, J, -J, K, -K, L, -L\}$, where I (for "identity") is, of course, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, and $-J$ is, for example, $\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$. To show that Q_8 is in fact a subgroup of $GL(2, \mathbb{C})$ it suffices to check that Q_8 is closed under matrix multiplication and inverses. Closure under multiplication follows from the facts that

Closed Inverses

$$J^2 = K^2 = L^2 = -I$$

and $KJ = -L$, $JK = L$, $KL = J$, $LK = -J$, $JL = -K$, $LJ = K$. Closure under inverses follows from the fact that $J^{-1} = -J$, $K^{-1} = -K$, and $L^{-1} = -L$. [For example, $J(-J) = -J^2 = -(-I) = I$.] However, it turns out that because Q_8 is a *finite* subset of $GL(2, \mathbb{C})$ it was really enough to check just closure under multiplication.

Thus Q_8 provides a nice illustration of the following elegant little theorem.

$(\mathbb{R}\setminus\{0\}, \times) \subset (\mathbb{C}\setminus\{0\}, \times)$

subset

a group

So this is a subgroup.

$$GL(2,\mathbb{C}) = \left\{ \begin{pmatrix} a_1 + a_2 i & b_1 + b_2 i \\ c_1 + c_2 i & d_1 + d_2 i \end{pmatrix} : \text{invertible} \right\}$$

Quaternion Group

$$Q_8 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} \right\}$$

$$Q_8 = \{I, J, K, L, -I, -J, -K, -L\}$$

A subgroup. See book for proof.

$\boxed{\text{Review}}$

Given $a \in G$

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

Example $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \in GL(2, \mathbb{R})$

Find $\left\langle \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$ Check this is a subgroup

$\boxed{\text{HW2}}$ Let $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in GL(2, \mathbb{R})$

Find $\left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \right\rangle$

Check this is a subgroup

$\boxed{\text{Thm}}$ Let G be any group and let $a \in G$. Then $\langle a \rangle$ is a subgroup of G. For clearly $\langle a \rangle \neq \varnothing$, and $\langle a \rangle$ is closed under multiplication since if $a^j, a^k \in \langle a \rangle$ then $a^j a^k = a^{j+k} \in \langle a \rangle$. Finally, $\langle a \rangle$ is closed under inverses since if $a^j \in \langle a \rangle$ then $(a^j)^{-1} = a^{-j} \in \langle a \rangle$.

Klein 4 group

3. Let's find all the subgroups of Klein's 4-group, $V = \{e, a, b, c\}$ with $a^2 = b^2 = c^2 = e$, $ab = ba = c$, $ac = ca = b$, $bc = cb = a$. The only subgroup that contains none of a, b, or c is obviously $\{e\}$. If a subgroup contains just one of a, b, or c then it is either $\langle a \rangle$, $\langle b \rangle$, or $\langle c \rangle$. If it contains two of a, b, c then by the definition of multiplication in V, it contains the third as well, and since it contains e it must then be V. Thus the subgroups are $\langle e \rangle$, $\langle a \rangle$, $\langle b \rangle$, $\langle c \rangle$, and V.

Klein's 4-group is thus an example of an abelian noncyclic group with the property that all of its proper subgroups are cyclic. (A subgroup H of G is **proper** if $H \neq G$.)

We sometimes make a schematic picture of the subgroups of a group by drawing what is called a **subgroup lattice**. The subgroup lattice for Klein's

---

Example $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \in GL(2, \mathbb{R})$

$\left\langle \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle =$

$= \left\{ \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^0, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^1, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^2, \dots \right.$

$\left. \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{-1}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{-2}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{-3} \dots \right\}$

$= \left\{ I, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 8 & 0 \\ 0 & 1 \end{pmatrix} \dots \right.$

$\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1/4 & 0 \\ 0 & 1 \end{pmatrix}, \dots$

$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix}$

$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^3 = \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 8 & 0 \\ 0 & 1 \end{pmatrix}$

$\left(\begin{array}{cc|cc} 2 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{array}\right) \to \left(\begin{array}{cc|cc} 1 & 0 & 1/2 & 0 \\ 0 & 1 & 0 & 1 \end{array}\right)$

$\begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1/4 & 0 \\ 0 & 1 \end{pmatrix}$

Lesson 10

SUBGROUPS

Review $(G,*)$ is a group if it is

- a binary operation $a,b \in G \Rightarrow a*b \in G$
- associative $\forall a,b,c \in G$ $a*(b*c) = (a*b)*c$
- has an identity e $e*a = a*e = a$ $\forall a \in G$
- each element $a \in G$ has an inverse $a^{-1} \in G$ s.t $a*a^{-1} = a^{-1}*a = e$.

DEFINITION A subset H of a group $(G,*)$ is called a **subgroup** of G if the elements of H form a group under $*$.

$2\mathbb{Z}$ = even integers
$(2\mathbb{Z},+)$ is a subgroup of $(\mathbb{Z},+)$

$\left\{\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a,b,c \in \mathbb{R}\right\}$ is a subgroup of $GL(3,\mathbb{R})$ with matrix mult.

THEOREM 5.1 Let H be a nonempty subset of a group G. Then H is a subgroup of G if and only if the following two conditions are satisfied:

i) for all $a,b \in H$, $ab \in H$, (closed under $*$)
ii) for all $a \in H$, $a^{-1} \in H$. (closed under inverses)

Proof (on right)

$\boxed{\text{HW1}}$ Use Thm 5.1 to prove $\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| ad-bc=1\right\}$ is a subgroup of $GL(2,\mathbb{R})$

$\left\langle \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 2^n & 0 \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z} \right\}$

$1, 2, 4, 8$
$\frac{1}{2}$ $\frac{1}{4}$

these are invertible so $\subset GL(2,\mathbb{R})$

Check this is a subgroup of $GL(2,\mathbb{R})$

- Closed under matrix mult:

① Given $a,b \in \left\langle \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$ $\exists n,m \in \mathbb{Z}$ s.t $a = \begin{pmatrix} 2^n & 0 \\ 0 & 1 \end{pmatrix}$ $b = \begin{pmatrix} 2^m & 0 \\ 0 & 1 \end{pmatrix}$ — ① by our $\left\langle \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$

② $a*b = \begin{pmatrix} 2^n & 0 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 2^m & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2^n 2^m & 0 \\ 0 & 1\cdot 1 \end{pmatrix}$ — ② by defn matrix mult

③ $= \begin{pmatrix} 2^{n+m} & 0 \\ 0 & 1 \end{pmatrix} \in \left\langle \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$ — ③ by $2^n 2^m = 2^{n+m}$ and defn of our set.

- Closed under inverses:

① Given $a \in \left\langle \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$ $\exists n \in \mathbb{Z}$ s.t $a = \begin{pmatrix} 2^n & 0 \\ 0 & 1 \end{pmatrix}$ — ① by defn of set

② Let $a^{-1} = \begin{pmatrix} 2^{-n} & 0 \\ 0 & 1 \end{pmatrix} \in \left\langle \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$ — ② by defn of set $n \in \mathbb{Z} \Rightarrow -n \in \mathbb{Z}$

③ Check $a*a^{-1} = \sim\sim\sim = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ — ③ matrix mult.

3:34 AM Sun Sep 27

Abstract_Algebra_1-5

Modern Algebra & Number Systems | Abstract_Algebra_1-5

THEOREM 5.1 Let H be a nonempty subset of a group G. Then H is a subgroup of G if and only if the following two conditions are satisfied:

i) for all $a, b \in H$, $ab \in H$, (closed under $*$)

ii) for all $a \in H$, $a^{-1} \in H$. (closed under inverses)

Proof (on right)

$\boxed{\text{HW1}}$ Use Thm 5.1 to prove $\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| ad-bc=1\right\}$ is a subgroup of $GL(2,\mathbb{R})$

$\boxed{\text{Review:}}$

Given $a \in G$

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

Example. $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \in GL(2,\mathbb{R})$

Find $\left\langle \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$ Check this is a subgroup

$\boxed{\text{HW2}}$ Let $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in GL(2,\mathbb{R})$

Find $\left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \right\rangle$

Check this is a subgroup

$\boxed{\text{Thm}}$ 2. Let G be any group and let $a \in G$. Then $\langle a \rangle$ is a subgroup of G. For clearly $\langle a \rangle \neq \varnothing$, and $\langle a \rangle$ is closed under multiplication since if $a^j, a^k \in \langle a \rangle$ then $a^j a^k = a^{j+k} \in \langle a \rangle$. Finally, $\langle a \rangle$ is closed under inverses since if $a^j \in \langle a \rangle$ then $(a^j)^{-1} = a^{-j} \in \langle a \rangle$.

Klein 4 group

3. Let's find all the subgroups of Klein's 4-group, $V = \{e, a, b, c\}$ with $a^2 = b^2 = c^2 = e$, $ab = ba = c$, $ac = ca = b$, $bc = cb = a$. The only subgroup that contains none of a, b, or c is obviously $\{e\}$. If a subgroup contains just one of a, b, or c then it is either $\langle a \rangle$, $\langle b \rangle$, or $\langle c \rangle$. If it contains two of a, b, c then by

---

27%

Modern Algebra & Number Systems

Linear Algebra | Modern Algebra & Number Systems

<u>Thm</u> Given any group $(G,*)$ and any $a \in G$ the $\langle a \rangle$ is a subgroup of G

<u>Proof</u>:

$\langle a \rangle$ is a <u>nonempty</u> <u>subset</u> because $a \in \langle a \rangle$ and because $\langle a \rangle \subset G$ because G is a binary operation

<u>Closed under $*$</u>:

Given $g_1, g_2 \in \langle a \rangle$ Show $g_1 * g_2 \in \langle a \rangle$

$\exists n_1, n_2 \in \mathbb{Z}$ s.t $g_1 = a^{n_1}$ $g_2 = a^{n_2}$ by the defn of $\langle a \rangle$

$g_1 * g_2 = a^{n_1} * a^{n_2} = a^{n_1+n_2}$ by power addition thm

$g_1 * g_2 \in \langle a \rangle$ because $n_1 + n_2 \in \mathbb{Z}$.

<u>Closed under inverses</u>:

Given $g \in \langle a \rangle$ Show $g^{-1} \in \langle a \rangle$

$\exists n \in \mathbb{Z}$ s.t $g = a^n$

then $g^{-1} = a^{-n}$ by power inverse thm $g^{-1} \in \langle a \rangle$ because $-n \in \mathbb{Z}$.

QED

3:44 AM Sun Sep 27

Abstract_Algebra_1-5

Klein 4 group

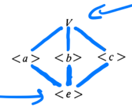
3. Let's find all the subgroups of Klein's 4-group, $V=\{e,a,b,c\}$ with $a^2=b^2=c^2=e$, $ab=ba=c$, $ac=ca=b$, $bc=cb=a$. The only subgroup that contains none of a, b, or c is obviously $\{e\}$. If a subgroup contains just one of a, b, or c then it is either $\langle a\rangle$, $\langle b\rangle$, or $\langle c\rangle$. If it contains two of a,b,c then by the definition of multiplication in V, it contains the third as well, and since it contains e it must then be V. Thus the subgroups are $\langle e\rangle$, $\langle a\rangle$, $\langle b\rangle$, $\langle c\rangle$, and V.

Klein's 4-group is thus an example of an abelian noncyclic group with the property that all of its proper subgroups are cyclic. (A subgroup H of G is **proper** if $H\neq G$.)

We sometimes make a schematic picture of the subgroups of a group by drawing what is called a **subgroup lattice**. The subgroup lattice for Klein's

Subgroup Lattice

4-group is



subgroups that contain them

the next smallest that include $\langle e\rangle$

$\langle e\rangle$

A line going upward from one group to another indicates that the bottom group is a subgroup of the top one.

$\boxed{HW3}$ Write the table for $\mathbb{Z}_3$ and find $\langle 0\rangle$ $\langle 1\rangle$ $\langle 2\rangle$ and draw the subgroup lattice.

$\boxed{HW4}$ Write the table for $\mathbb{Z}_4$ and find $\langle 0\rangle$ $\langle 1\rangle$ $\langle 2\rangle$ $\langle 3\rangle$ and draw the subgroup lattice.

Modern Algebra & Number Systems

24%

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Klein 4 group table

$(V, *)$

List the subgroups

$\{e\} = \langle e\rangle$

$\langle a\rangle = \{e, a\}$ because $a^2=e$ $a^{-1}=a$

$\langle b\rangle = \{e, b\}$ because $b^2=e$ $b^{-1}=b$

$\langle c\rangle = \{e, c\}$ because $c^2=e$ $c^{-1}=c$

Are these subsets subgroups?

$\{e, a, b\}$? No $a*b=c$ Not closed under $*$

$\{e, b, c\}$? No $b*c=a$

$\{e, a, c\}$? No $a*c=b$

Last subgroup is V itself.

groups

$\boxed{\text{HW5}}$ Read the proof and write in 2 columns

THEOREM 5.2 Let G be a cyclic group. Then every subgroup of G is cyclic.

PROOF. Suppose $G=\langle x\rangle$, and let H be a subgroup of G. If $H=\{e\}$, then clearly H is cyclic, so assume $H\neq\{e\}$. Let n be the smallest positive integer such that $x^n\in H$. (Why does n exist?) We assert that $H=\langle x^n\rangle$. For if $h\in H$ then $h=x^m$ for some integer m, because $h\in G=\langle x\rangle$. Write $m=qn+r$ where $0\leqslant r<n$. Then

$$h=x^{qn+r}=x^{qn}x^r=(x^n)^q x^r, \quad \text{and} \quad (x^n)^q\in H.$$

Read

Proof

So $x^r=x^{-nq}h\in H$. Since $0\leqslant r<n$, the definition of n implies that $r=0$, so $m=qn$ and

$$h=x^m=(x^n)^q\in\langle x^n\rangle.$$

Thus $H\subseteq\langle x^n\rangle$, and since it is obvious that $\langle x^n\rangle\subseteq H$, the proof is complete. □

It is often true in mathematics that the *proof* of a theorem contains substantially more information than the statement of the theorem itself. Theorem 5.2 is a case in point, and you are urged to study the proof carefully. For example, the proof tells us not only that every subgroup is cyclic, but also how to find a generator for each one.

There are, of course, questions about the subgroups of $(\mathbb{Z}_n,\oplus)$ that are left unanswered by this theorem. Which of $\langle 0\rangle,\langle 1\rangle,\langle 2\rangle,\ldots,\langle n-1\rangle$ coincide? How many distinct subgroups does $(\mathbb{Z}_n,\oplus)$ have? We shall return to these questions after we consider some more examples of subgroups.

Examples (continued)

6 Let G be the group of real-valued functions on the real line, under addition of functions, and let H be the set of continuous functions in G. Then H is a subgroup of G since the sum of two continuous functions is continuous (closure of H under addition of functions) and if f is continuous, then $-f$ is continuous (closure of H under inverses).

$G=(\mathbb{Z}_{12},\oplus)$

$11+1 \bmod 12 = 0$

$\langle 0\rangle=\{0\}$

$-1=11$

$\langle 1\rangle=\{0,1,2,3,4,5,6,7,8,9,10,11\}$

$\langle 2\rangle=\{0,2,4,6,8,10\}$ $\quad -2=10$

$\langle 3\rangle=\{0,3,6,9\}$

15 mod 12

$\langle 4\rangle=\{0,4,8\}$

13 mod 12

14 mod 12

$\langle 5\rangle=\{0,5,10,3,8,1,6,11,2,7\}$

$\langle 6\rangle=\{0,6\}$

$\langle 7\rangle=\{0,7,2,9,4,11,6,1,8,3,10,5\}$

$\langle 8\rangle=\{0,8,4\}$

$\langle 9\rangle=\{0,9,6,3\}$

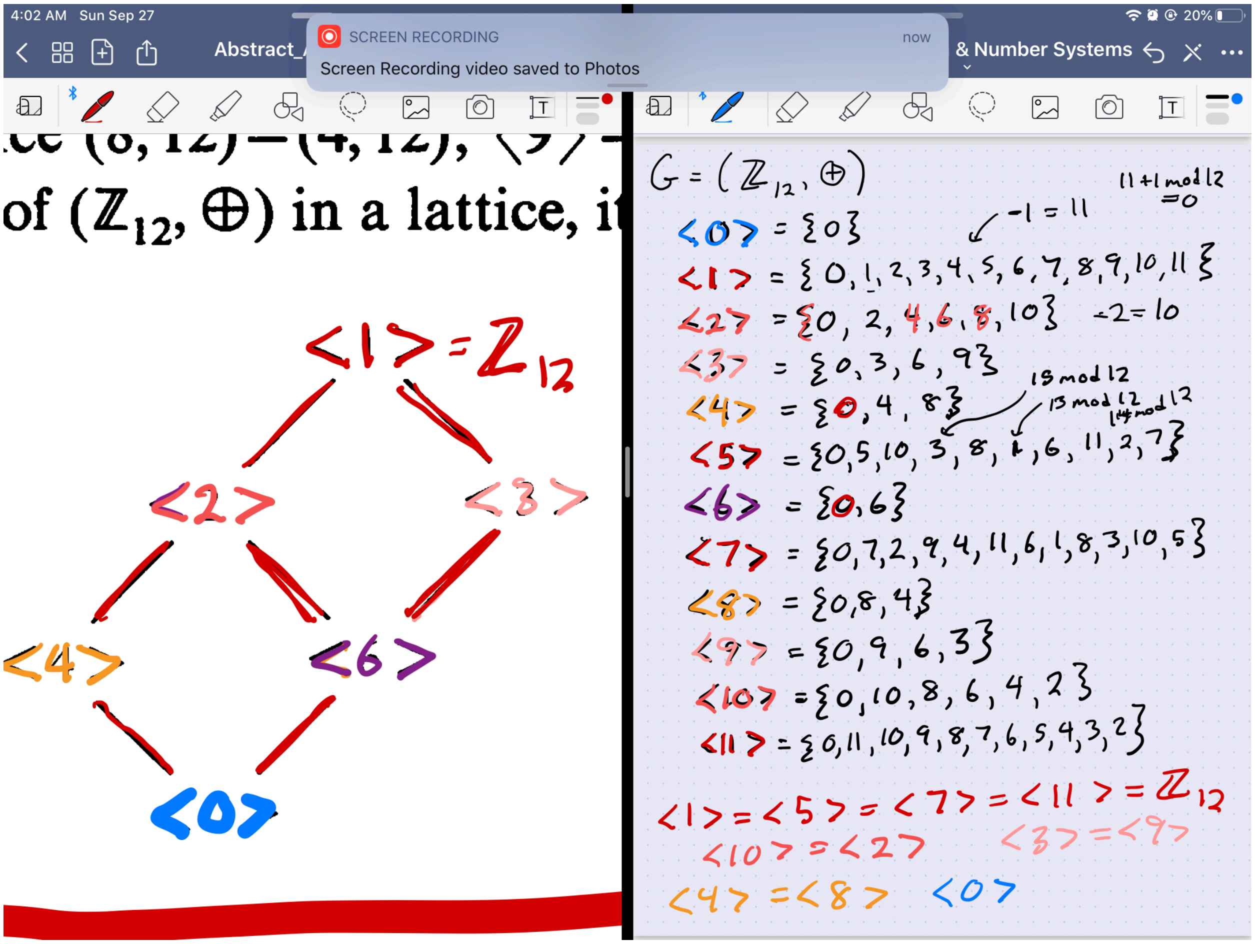
$\langle 10\rangle=\{0,10,8,6,4,2\}$

$\langle 11\rangle=\{0,11,10,9,8,7,6,5,4,3,2\}$

$\langle 1\rangle=\langle 5\rangle=\langle 7\rangle=\langle 11\rangle=\mathbb{Z}_{12}$

$\langle 10\rangle=\langle 2\rangle$ $\quad \langle 3\rangle=\langle 9\rangle$

$\langle 4\rangle=\langle 8\rangle$ $\quad \langle 0\rangle$



Note that in the lattice you don't repeat a subgroup. For example above we only have <4> and don't mention <8> which equals <4>.

Do HW1-HW5 (if you are behind schedule you may skip HW5)

Part 2:
Required for MAT615 and extra credit for MAT314:

Watch [Video 314F20-10-9] and [Video 314F20-10-10]

and $\ldots)\cdot(1/d)\neq 0$.

8. If G is any group, then the **center** of G, denoted by $Z(G)$, is the subset consisting of those elements that commute with everything in G. Thus

$$Z(G)=\{z\in G \mid zx=xz \quad \text{for all } x\in G\}.$$

(The Z comes from the German word "Zentrum.")

$\boxed{\text{HW6}}$ Prove the center is a subgroup.

Of course, if G is abelian, then $Z(G)=G$; but if G is nonabelian, then $Z(G)\subsetneq G$. As a specific example, let's try to figure out what the center of $GL(2,\mathbb{R})$ looks like.

Suppose $\begin{pmatrix} a & b\\ c & d\end{pmatrix}$ commutes with everything in $GL(2,\mathbb{R})$. Then since $\begin{pmatrix} 0 & 1\\ 1 & 0\end{pmatrix}\in GL(2,\mathbb{R})$, we have

$$\begin{pmatrix} a & b\\ c & d\end{pmatrix}\begin{pmatrix} 0 & 1\\ 1 & 0\end{pmatrix}=\begin{pmatrix} 0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix} a & b\\ c & d\end{pmatrix},$$

that is,

$$\begin{pmatrix} b & a\\ d & c\end{pmatrix}=\begin{pmatrix} c & d\\ a & b\end{pmatrix}.$$

This means that $a=d$ and $b=c$, so

$$\begin{pmatrix} a & b\\ c & d\end{pmatrix}=\begin{pmatrix} a & b\\ b & a\end{pmatrix}.$$

Furthermore, since $\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}\in GL(2,\mathbb{R})$, we also have

$$\begin{pmatrix} a & b\\ b & a\end{pmatrix}\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}=\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix} a & b\\ b & a\end{pmatrix},$$

that is,

$$\begin{pmatrix} a & a+b\\ b & b+a\end{pmatrix}=\begin{pmatrix} a+b & b+a\\ b & a\end{pmatrix}.$$

Thus $b=0$, so every element of the center has the form $\begin{pmatrix} a & 0\\ 0 & a\end{pmatrix}$, $a\neq 0$. It is easy to see that, conversely, all elements of this form are in the center, so

$$Z(GL(2,\mathbb{R}))=\left\{\begin{pmatrix} a & 0\\ 0 & a\end{pmatrix} \middle| a\neq 0\right\}.$$

In this case the center is clearly a subgroup, and it is not hard to see that the center is *always* a subgroup, no matter what group G is (Exercise 5.22).

9. Let $G=GL(2,\mathbb{C})$, the general linear group of degree two over the complex numbers. This is the set of all invertible matrices

$$\begin{pmatrix} a_1+a_2 i & b_1+b_2 i\end{pmatrix}$$

Lesson 9 Part 2

Given a group G the center of G $Z(G)$

$Z(G)=\{z \mid \forall x\in G \;\; zx=xz\}\subset G$

Example What is the center of $GL(2,\mathbb{R})=G$?

$$Z(G)=\left\{\begin{pmatrix} z_{11} & z_{12}\\ z_{21} & z_{22}\end{pmatrix} \middle| \forall \begin{pmatrix} x_{11} & x_{12}\\ x_{21} & x_{22}\end{pmatrix}\in GL(2,\mathbb{R}) \;\; \begin{pmatrix} z_{11} & z_{12}\\ z_{21} & z_{22}\end{pmatrix}\begin{pmatrix} x & -\\ - & -\end{pmatrix}=\begin{pmatrix} x & -\\ - & -\end{pmatrix}\begin{pmatrix} z & -\\ - & -\end{pmatrix}\right\}$$

book $\begin{pmatrix} a & b\\ c & d\end{pmatrix}$

try various

$$\begin{pmatrix} x_{11} & x_{12}\\ x_{21} & x_{22}\end{pmatrix}=\begin{pmatrix} 0 & 1\\ 1 & 0\end{pmatrix},$$

$$\begin{pmatrix} x_{11} & x_{12}\\ x_{21} & x_{22}\end{pmatrix}=\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}$$

and ... $)\cdot(1/d)\neq 0$.

8. If G is any group, then the **center** of G, denoted by $Z(G)$, is the subset consisting of those elements that commute with everything in G. Thus

$$Z(G)=\{z\in G \mid zx=xz \quad \text{for all } x\in G\}.$$

(The Z comes from the German word "Zentrum.")

$\boxed{\text{HW6}}$ Prove the center is a subgroup.

Of course, if G is abelian, then $Z(G)=G$; but if G is nonabelian, then $Z(G)\subsetneq G$. As a specific example, let's try to figure out what the center of $GL(2,\mathbb{R})$ looks like.

Suppose $\begin{pmatrix} a & b\\ c & d\end{pmatrix}$ commutes with everything in $GL(2,\mathbb{R})$. Then since $\begin{pmatrix} 0 & 1\\ 1 & 0\end{pmatrix}\in GL(2,\mathbb{R})$, we have

$$\begin{pmatrix} a & b\\ c & d\end{pmatrix}\begin{pmatrix} 0 & 1\\ 1 & 0\end{pmatrix}=\begin{pmatrix} 0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix} a & b\\ c & d\end{pmatrix},$$

that is,

$$\begin{pmatrix} b & a\\ d & c\end{pmatrix}=\begin{pmatrix} c & d\\ a & b\end{pmatrix}.$$

This means that $a=d$ and $b=c$, so

$$\begin{pmatrix} a & b\\ c & d\end{pmatrix}=\begin{pmatrix} a & b\\ b & a\end{pmatrix}.$$

Furthermore, since $\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}\in GL(2,\mathbb{R})$, we also have

$$\begin{pmatrix} a & b\\ b & a\end{pmatrix}\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}=\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix} a & b\\ b & a\end{pmatrix},$$

that is,

$$\begin{pmatrix} a & a+b\\ b & b+a\end{pmatrix}=\begin{pmatrix} a+b & b+a\\ b & a\end{pmatrix}.$$

Thus $b=0$, so every element of the center has the form $\begin{pmatrix} a & 0\\ 0 & a\end{pmatrix}$, $a\neq 0$. It is easy to see that, conversely, all elements of this form are in the center, so

$$Z(GL(2,\mathbb{R}))=\left\{\begin{pmatrix} a & 0\\ 0 & a\end{pmatrix}\,\middle|\, a\neq 0\right\}.$$

Example What is the center of $GL(2,\mathbb{R})=G$?

$$Z(G)=\left\{\begin{pmatrix} z_{11} & z_{12}\\ z_{21} & z_{22}\end{pmatrix} \,\middle|\, \forall \begin{pmatrix} x_{11} & x_{12}\\ x_{21} & x_{22}\end{pmatrix}\in GL(2,\mathbb{R}) \quad \begin{pmatrix} z_{11} & z_{12}\\ z_{21} & z_{22}\end{pmatrix}\begin{pmatrix} x & \\ & \end{pmatrix}=\begin{pmatrix} x & \\ & \end{pmatrix}\begin{pmatrix} z & \\ & \end{pmatrix}\right\}$$

book $\begin{pmatrix} a & b\\ c & d\end{pmatrix}$

try various $\begin{pmatrix} x_{11} & x_{12}\\ x_{21} & x_{22}\end{pmatrix}=\begin{pmatrix} 0 & 1\\ 1 & 0\end{pmatrix}$,

$$\begin{pmatrix} x_{11} & x_{12}\\ x_{21} & x_{22}\end{pmatrix}=\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}$$

Try $\begin{pmatrix} a & 0\\ 0 & a\end{pmatrix}\begin{pmatrix} x_{11} & x_{12}\\ x_{21} & x_{22}\end{pmatrix}=\begin{pmatrix} ax_{11} & ax_{12}\\ ax_{21} & ax_{22}\end{pmatrix}$

$$\begin{pmatrix} x_{11} & x_{12}\\ x_{21} & x_{22}\end{pmatrix}\begin{pmatrix} a & 0\\ 0 & a\end{pmatrix}=\begin{pmatrix} x_{11}a & x_{12}a\\ x_{21}a & x_{22}a\end{pmatrix}$$

match

$\forall x\in G$

$\boxed{\text{HW6}}$

Given $Z(G) \subset G$

$\forall x \in G$
$x(z_1 z_2) = (z_1 z_2)x$

• closed under $*$

Given $z_1, z_2 \in Z(G)$

Show $z_1 z_2 \in Z(G)$

① $xz_1 = z_1 x \quad \forall x \in G$ ① by defn of $Z(G)$

$xz_2 = z_2 x \quad \forall x \in G$

② $x(z_1 z_2) = (xz_1)z_2$

③ $= (z_1 x) z_2$

④ $= z_1(xz_2)$

⑤ $= z_1(z_2 x)$

⑥ $(z_1 z_2)x =$

⑦⑧⑨

Show the sp match

⑩ $z_1 z_2 \in Z(G)$ ④ by ~~steps 2-9~~ matching & defn of center.

• closed under inverses

Given: $z \in Z(G)$ $\quad \forall x \in G \; xz = zx$

Show: $z^{-1} \in Z(G)$ $\quad \forall x \in G \; xz^{-1} = z^{-1}x$

Very tricky

5.8 Let $G=\langle x\rangle$ be a cyclic group of order 144. How many elements are there in the subgroup $\langle x^{26}\rangle$?

5.9 Let $m\mathbb{Z}$ and $n\mathbb{Z}$ be subgroups of $(\mathbb{Z},+)$. What condition on m and n is equivalent to $m\mathbb{Z}\subseteq n\mathbb{Z}$? What condition on m and n is equivalent to $m\mathbb{Z}\cup n\mathbb{Z}$ being a subgroup of $(\mathbb{Z},+)$?

5.10 Prove that every subgroup of an abelian group is abelian.

5.11 Let G be an abelian group, and let n be a positive integer. Let H be the subset of G consisting of all $x\in G$ such that $x^n=e$. Show that H is a subgroup of G.

5.12 Find the center of:

a) V;

b) Q_8.

5.13 Let H be the group introduced in Example 7 on p. 46. Find $Z(H)$.

HW 7

5.14 Prove that the intersection of two subgroups of a group G is itself a subgroup of G.

5.15 Show that if H and K are subgroups of the group G, then $H\cup K$ is closed under inverses.

5.16 Give an example of a group G and a subset H of G such that H is closed under multiplication but H is *not* a subgroup of G.

5.17 Suppose H is a nonempty finite subset of a group G and H is closed under inverses. Must H be a subgroup of G? Either prove that it must, or give a counterexample.

5.18 a) Show that it is impossible for a group G to be the union of two proper subgroups.

b) Give an example of a group that is the union of three proper subgroups.

5.19 Let $G=\langle x\rangle$ be an infinite cyclic group. Show that all the distinct subgroups of G are $\langle e\rangle,\langle x\rangle,\langle x^2\rangle,\langle x^3\rangle,\langle x^4\rangle,\langle x^5\rangle,\ldots$.

5.20 Let G be a finite group with no subgroups other than $\{e\}$ or G itself. Prove that G is either the trivial group $\{e\}$ or a cyclic group of prime order.

5.21 Let $G=\langle x\rangle$ be a cyclic group of order n. Find a condition on the integers r and s that is equivalent to $\langle x^r\rangle\subseteq\langle x^s\rangle$.

5.22 Let G be a group. Prove that $Z(G)$ is a subgroup of G. ← HW6

5.23 Let G be a group, and let $g\in G$. Define the centralizer, $Z(g)$, of g in G to be the subset

$$Z(g)=\{x\in G \mid xg=gx\}.$$ ← HW8

Prove that $Z(g)$ is a subgroup of G.

5.24 Let G be a group and let H be a nonempty subset of G such that whenever $x,y\in H$ we have $xy^{-1}\in H$. Prove that H is a subgroup of G.

HW 7

Given H_1, H_2 are subgroups of G

Show $H = H_1 \cap H_2$ is a subgroup

Show Closed under $*$

Given $a, b \in H$ Show $a*b \in H$

① $a, b \in H = H_1 \cap H_2$ ① by defn of H

② $a, b \in H_1$ AND $a, b \in H_2$ ② by defn of intersection

③ $a*b \in$ __ AND $a*b \in$ __ ③ H_1, H_2 are subgroups

④ ⑤ $a*b \in H$ ← goal

Show Closed under inverses

Given: Show:

①

⋮

⑤

QED

5:05 AM Sun Sep 27

Abstract_Algebra_1-5

Abstract_Algebra_1-5 | Modern Algebra & Number Systems

5.21 Let $G=\langle x\rangle$ be a cyclic group of order n. Find a condition on the integers r and s that is equivalent to $\langle x^r\rangle \subseteq \langle x^s\rangle$.

5.22 Let G be a group. Prove that $Z(G)$ is a subgroup of G. HW6

5.23 Let G be a group, and let $g \in G$. Define the centralizer, $Z(g)$, of g in G to be the subset

$$Z(g)=\{x\in G \mid xg=gx\}.$$

C HW8

Prove that $Z(g)$ is a subgroup of G.

5.24 Let G be a group and let H be a nonempty subset of G such that whenever $x,y\in H$ we have $xy^{-1}\in H$. Prove that H is a subgroup of G.

HW9

5.25 Let G be a group and let a be some fixed element of G. Let H be a subgroup of G and let aHa^{-1} be the subset of G consisting of all elements that are of the form aha^{-1}, with $h\in H$. Show that aHa^{-1} is a subgroup of G. It is called the *conjugate subgroup of H by a*.

5.26 Let H be a subgroup of the group G and let $N(H)=\{a\in G \mid aHa^{-1}=H\}$. (See Exercise 5.25 for the definition of aHa^{-1}.) Prove that $N(H)$ is a subgroup of G.

5.27 Let G be a finite abelian group. Show that G is cyclic iff G has the property that for every positive integer n, there are at most n elements x in G such that $x^n=e$.

HW10

MAT314 students:
If you are behind
schedule you may
skip HW6-HW10.

MAT615
students
must do all

Modern Algebra & Number Systems

HW8 Given H is nonempty subset of G

$\forall x,y\in H$ $xy^{-1}\in H$

Show H is a subgroup

Proof (Plan)

Part III Show it is closed under $*$

Given: $a,b\in H$ Show $a*b\in H$

Hint $x=a$?! $y=b^{-1}$

Part II Show it is closed under inv

Given $a\in H$ Show $a^{-1}\in H$

try $y=a$ $x=e$

then $ey^{-1}=e\cdot a^{-1}=a^{-1}$.

Part I

First show $e\in H$ $y=x$ $xy^{-1}=xx^{-1}=e\in H$

5.21 Let $G=\langle x\rangle$ be a cyclic group of order n. Find a condition on the integers r and s that is equivalent to $\langle x^r\rangle\subseteq\langle x^s\rangle$.

5.22 Let G be a group. Prove that $Z(G)$ is a subgroup of G. $\boxed{HW6}$

5.23 Let G be a group, and let $g\in G$. Define the centralizer, $Z(g)$, of g in G to be the subset

$$Z(g)=\{x\in G\,|\,xg=gx\}.$$

$\boxed{HW8}$

Prove that $Z(g)$ is a subgroup of G.

5.24 Let G be a group and let H be a nonempty subset of G such that whenever $x,y\in H$ we have $xy^{-1}\in H$. Prove that H is a subgroup of G.

$\boxed{HW9}$

5.25 Let G be a group and let a be some fixed element of G. Let H be a subgroup of G and let aHa^{-1} be the subset of G consisting of all elements that are of the form aha^{-1}, with $h\in H$. Show that aHa^{-1} is a subgroup of G. It is called the *conjugate subgroup of H by a*.

5.26 Let H be a subgroup of the group G and let $N(H)=\{a\in G\,|\,aHa^{-1}=H\}$. (See Exercise 5.25 for the definition of aHa^{-1}.) Prove that $N(H)$ is a subgroup of G.

5.27 Let G be a finite abelian group. Show that G is cyclic iff G has the property that for every positive integer n, there are at most n elements x in G such that $x^n=e$.

$\boxed{HW10}$

MAT314 students:
If you are behind schedule you may skip HW6-HW10.

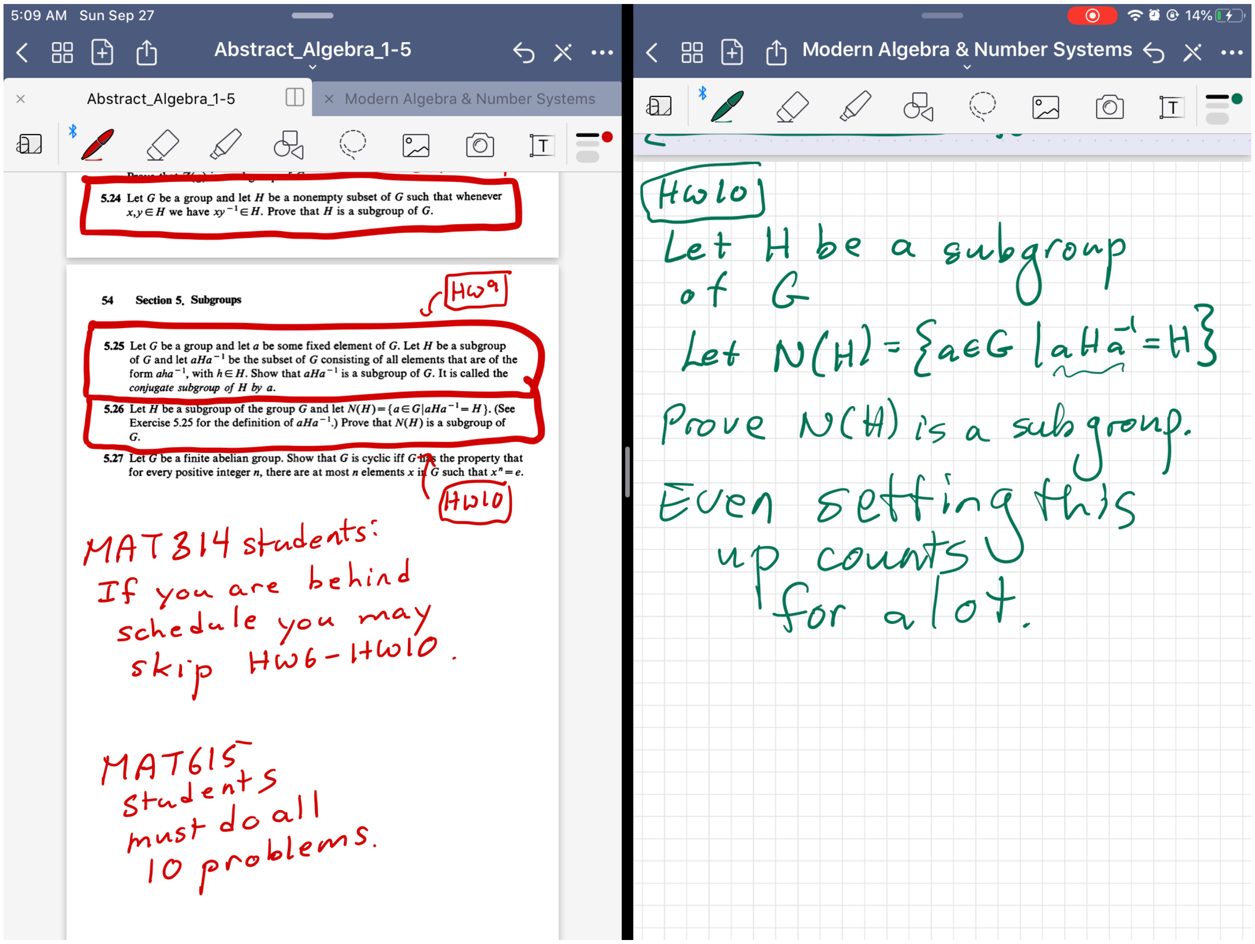
MAT615 students must do all

$\boxed{HW9}$ H a subgroup of G
$a\in G$
$aHa^{-1}=\{aha^{-1}\mid h\in H\}\in G$

Show aHa^{-1} is a subgroup

Maybe explore
check out the subgroups in $\mathbb{Z}_{12}$
$H=\langle 4\rangle$
$a=3$
$aHa^{-1}=?$

closed under $*$
closed under inverses
Set up



5.24 Let G be a group and let H be a nonempty subset of G such that whenever $x, y \in H$ we have $xy^{-1} \in H$. Prove that H is a subgroup of G.

54 **Section 5. Subgroups**

HW9

5.25 Let G be a group and let a be some fixed element of G. Let H be a subgroup of G and let aHa^{-1} be the subset of G consisting of all elements that are of the form aha^{-1}, with $h \in H$. Show that aHa^{-1} is a subgroup of G. It is called the *conjugate subgroup of H by a*.

5.26 Let H be a subgroup of the group G and let $N(H) = \{a \in G \mid aHa^{-1} = H\}$. (See Exercise 5.25 for the definition of aHa^{-1}.) Prove that $N(H)$ is a subgroup of G.

5.27 Let G be a finite abelian group. Show that G is cyclic iff G has the property that for every positive integer n, there are at most n elements x in G such that $x^n = e$.

HW10

MAT314 students:
If you are behind schedule you may skip HW6-HW10.

MAT615 students must do all 10 problems.

HW10

Let H be a subgroup of G

Let $N(H) = \{a \in G \mid aHa^{-1} = H\}$

Prove $N(H)$ is a subgroup.

Even setting this up counts for a lot.

For HW9 and HW10, please send me your given and show for your two oroofs before doing the proofs. Also since the variable a is used in the defns of these sets use x and y as sample points in the subgroup for the closure under * and for inverses.