35003 MODERN ALGEBRA

Prof Murray Elder, UTS

Week 2: subgroup, coset, normal subgroups, homomorphism

Lauritzen 2.2, 2.3, 2.4, 2.5

Definition (2.2.1)

A subgroup of G is a non-empty subset $H \subseteq G$ such that the composition of G makes H into a group.

Claim (quick proof in your head): $H \subseteq G$ is a subgroup of G if and only if

1. $e \in H$
2. $x^{-1} \in H$ for every $x \in H$
3. $xy \in H$ for every $x, y \in H$.

— Proposition.

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

Definition (2.2.1)

A subgroup of G is a non-empty subset $H \subseteq G$ such that the composition of G makes H into a group.

Claim (quick proof in your head): $H \subseteq G$ is a subgroup of G if and only if

1. $e \in H$
2. $x^{-1} \in H$ for every $x \in H$
3. $xy \in H$ for every $x, y \in H$.

Eg: the matrices of the form $\begin{bmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ are a subgroup of $\mathcal{H}_3$.

worksheet 1

PROP 2.2.3

The only subgroups of $(\mathbb{Z}, +)$ are

$$H = d\mathbb{Z} = \{dn \mid n \in \mathbb{Z}\} = \{\dots, -2d, -d, 0, d, 2d, \dots\}$$

Proof: simple number theory (check it).

Definition

Let H be a subgroup of G and $g \in G$.

The subset $gH = \{gh \mid h \in H\} \subseteq G$ is it a subgroup?

$e \in H$

$e \in gH$?

$gh \stackrel{?}{=} e$?

$g^{-1} g h = g^{-1} e$

$h = g^{-1}$

$g = h^{-1}$

$g \in H$.

COSET

Definition

Let H be a subgroup of G and $g \in G$.

The subset $gH = \{gh \mid h \in H\} \subseteq G$ is it a subgroup? only when $g \in H$
is called a *left coset* of H.

COSET

Definition

Let H be a subgroup of G and $g \in G$.

The subset $gH = \{gh \mid h \in H\} \subseteq G$ is it a subgroup? only when $g \in H$
is called a *left coset* of H.

The subset $Hg = \{hg \mid h \in H\} \subseteq G$ is called a *right coset* of H.

Definition

Let H be a subgroup of G and $g \in G$.

The subset $gH = \{gh \mid h \in H\} \subseteq G$ is it a subgroup? only when $g \in H$
is called a *left coset* of H.

The subset $Hg = \{hg \mid h \in H\} \subseteq G$ is called a *right coset* of H.

The **set** of left cosets of H is denoted G/H (and right cosets $H\backslash G$).

$\mathbb{Z}$, $H = 6\mathbb{Z}$

$6\mathbb{Z}$

$gH = 1 + 6\mathbb{Z}$ $\{ \ldots, -5, 1, 7, 13, \ldots \}$

$2 + 6\mathbb{Z}$

$\ldots$ $5 + 6\mathbb{Z}$

$\mathbb{Z}/6\mathbb{Z} = \{0 + 6\mathbb{Z}, 1 + 6\mathbb{Z}, \ldots, 5 + 6\mathbb{Z}\} = \{[0], [1], \ldots, [5]\}$

Definition

Let H be a subgroup of G and $g \in G$.

The subset $gH = \{gh \mid h \in H\} \subseteq G$ is it a subgroup? only when $g \in H$
is called a *left coset* of H.

The subset $Hg = \{hg \mid h \in H\} \subseteq G$ is called a *right coset* of H.

The **set** of left cosets of H is denoted G/H (and right cosets $H\backslash G$).

Ex: let $G = GL_2(\mathbb{R}), H = SL_2(\mathbb{R})$ (all 2×2 real matrices with determinant 1)

det ≠ 0

subgroup

Definition

Let H be a subgroup of G and $g \in G$.

The subset $gH = \{gh \mid h \in H\} \subseteq G$ is it a subgroup? only when $g \in H$
is called a *left coset* of H.

The subset $Hg = \{hg \mid h \in H\} \subseteq G$ is called a *right coset* of H.

The **set** of left cosets of H is denoted G/H (and right cosets $H\backslash G$).

Ex: let $G = GL_2(\mathbb{R}), H = SL_2(\mathbb{R})$ (all 2×2 real matrices with determinant 1)

(a) Give four elements of the left coset $\begin{pmatrix} 2.5 & 0 \\ 0 & 1 \end{pmatrix} H$.

Definition

Let H be a subgroup of G and $g \in G$.

The subset $gH = \{gh \mid h \in H\} \subseteq G$ is it a subgroup? only when $g \in H$
is called a *left coset* of H.

The subset $Hg = \{hg \mid h \in H\} \subseteq G$ is called a *right coset* of H.

The **set** of left cosets of H is denoted G/H (and right cosets $H \backslash G$).

Ex: let $G = GL_2(\mathbb{R}), H = SL_2(\mathbb{R})$ (all 2×2 real matrices with determinant 1)

(a) Give four elements of the left coset $\begin{pmatrix} 2.5 & 0 \\ 0 & 1 \end{pmatrix} \cdot H$.

(b) Give four elements of G/H.

H, $\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix} H$ ← not a new one!

MORE EXAMPLES OF COSETS

Compute the left and right cosets of $H = \{e, a\}$ in S_3 (Example 2.1.6).

subgroup

MORE EXAMPLES OF COSETS

Compute the left and right cosets of $H = \{e, a\}$ in S_3 (Example 2.1.6).

$$e = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \quad a = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}, \quad b = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix},$$
$$c = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}, \quad d = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}, \quad f = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}.$$

$\circ$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	f	d	c	b
b	b	d	e	f	a	c
c	c	f	d	e	b	a
d	d	b	c	a	f	e
f	f	c	a	b	e	d

$$a \cdot a = \begin{matrix}1 & 2 & 3\\ 2 & 1 & \downarrow\\ 1 & 2 & 3\end{matrix}$$

MORE EXAMPLES OF COSETS

Compute the left and right cosets of $H = \{e, a\}$ in S_3 (Example 2.1.6).

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$c = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

$\circ$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	f	d	c	b
b	b	d	e	f	a	c
c	c	f	d	e	b	a
d	d	b	c	a	f	e
f	f	c	a	b	e	d

$$\begin{aligned} eH &= \{ee, ea\} = \{e, a\}, \\ aH &= \{ae, aa\} = \{a, e\}, \\ bH &= \{be, ba\} = \{b, d\}, \\ cH &= \{ce, ca\} = \{c, f\}, \\ dH &= \{de, da\} = \{d, b\}, \\ fH &= \{fe, fa\} = \{f, c\}. \end{aligned}$$

$$\begin{aligned} He &= \{ee, ae\} = \{e, a\}, \\ Ha &= \{ea, aa\} = \{a, e\}, \\ Hb &= \{eb, ab\} = \{b, f\}, \\ Hc &= \{ec, ac\} = \{c, d\}, \\ Hd &= \{ed, ad\} = \{d, c\}, \\ Hf &= \{ef, af\} = \{f, b\}. \end{aligned}$$

left — all have same size — right

$xH = \{xh : h \in H\}$ left coset.

Lemma (2.2.6)

Let H be a subgroup of G and $x, y \in G$. Then

(i) $x \in xH$

(ii) $xH = yH$ *if and only if* $x^{-1}y \in H$

(iii) *if* $xH \neq yH$ *then they are disjoint (so the cosets form a partition of the set G)*

Pf: contrapositive.

(iv) $\varphi_x \colon H \to xH$ *defined by* $\varphi_x(h) = xh$ *is a bijection*

Proof (i) $e \in H$ since H subgroup,

$\therefore x \cdot e \in x \cdot H$

$x \cdot e = x$

(ii) Suppose $xH = yH$ $\exists h_1, h_2 \in H$

$xh_1 = yh_2$ $h_1 = x^{-1} y h_2$ $h_1 h_2^{-1} = x^{-1}y$

$\therefore x^{-1}y \in H$.

$\Leftarrow$

If $x^{-1}y \in H$

$x^{-1}y = h$ some $h \in H$

$y = xh$ and $x = yh^{-1}$

To show $xH = yH$ for some arbitrary p.

$\subseteq$ Let $p \in xH$

$p = xh_1 = yh^{-1}h_1 \in yH$

$\therefore xH \subseteq yH$.

$\supseteq$ let $q \in yH$.

$q = yh_2 = ~~y~~ \; xhh_2 \in xH$

$\therefore yH \subseteq xH$.

(iii) To show (contrapositive)

$xH \cap yH \neq \emptyset \rightarrow xH = yH$.

Let $p \in xH \cap yH$

then $p = xh_1 = yh_2$

$h_1 = x^{-1}yh_2$

$h_1h_2^{-1} = x^{-1}y$

$\therefore x^{-1}y \in H$

$\therefore$ by (ii) $xH = H$.

(iv) $\varphi_x : H \to xH$ is bij.

1-1 : Suppose $\varphi_x(h_1) = \varphi_x(h_2)$

$$\begin{array}{ccc} \varphi_x(h_1) & = & \varphi_x(h_2) \\ \| & & \| \\ xh_1 & & xh_2 \end{array}$$

$$x^{-1}xh_1 = x^{-1}xh_2$$

$$\vdots$$

$$\therefore h_1 = h_2$$

onto: $\forall p \in xH$, $p = xh$ some $h \in H$

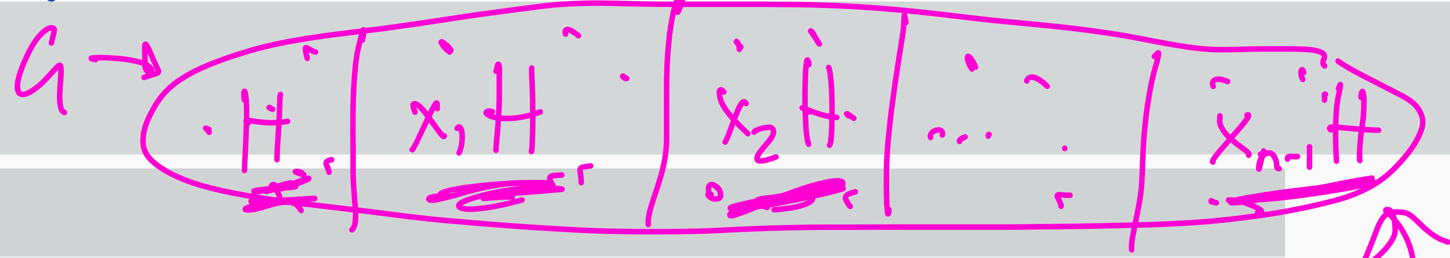
so $\exists h \,(= x^{-1}p)$

so that $\varphi_x(h) = xh = p$.

---

y

LAGRANGE



Lemma (2.2.6)

Let H be a subgroup of G and $x, y \in G$. Then

(i) $x \in xH$

(ii) $xH = yH$ *if and only if* $x^{-1}y \in H$

(iii) *if* $xH \neq yH$ *then they are disjoint (so the cosets form a partition of the set* G*)*

(iv) $\varphi_x : H \to xH$ *defined by* $\varphi_x(h) = xh$ *is a bijection*

After observing these facts, we can immediately get Lagrange's theorem (note Lagrange proved this before groups were formalised!)
Define $[G : H] = |G/H|$ called the *index* of G in H.

Theorem (2.2.8, Lagrange)

If $H \subseteq G$ is a subgroup of a finite group G, then $|G| = [G : H]|H|$.

Proof: draw the partition.

"Wouldn't it be nice if G/H was a group?"

What would the composition be?

$xH \circ yH = ?$

Wouldn't it be nice if $xHyH = \{xh_1yh_2 \mid h_1, h_2 \in H\}$ was actually the same set as $(xy)H$?

If so, then (Corollary 2.3.3) G/H with this composition forms a group (identity is H, etc).

(Note: for any subsets X, Y of a group G we can define $XY = \{xy \mid x \in X, y \in Y\}$ as a standard construction)

Wouldn't it be nice if $xHyH = \{xh_1yh_2 \mid h_1, h_2 \in H\}$ was actually the same set as $(xy)H$?

Not true for the subgroup $\{e, a\}$ of S_3 (check it).

$$(bH)(cH) = \{f, c, a, e\}.$$

not a coset.

Wouldn't it be nice if $xHyH = \{xh_1yh_2 \mid h_1, h_2 \in H\}$ was actually the same set as $(xy)H$?

Not true for the subgroup $\{e, a\}$ of S_3 (check it).

$$(bH)(cH) = \{f, c, a, e\}.$$

$(gh_1 = h_2 g)$

Proposition (2.3.1)

Let H be a subgroup of G. If $gH = Hg$ for all $g \in G$, then

$$(xH)(yH) = (xy)H$$

for all x, y in G.

Proof: two inclusions.

$\subseteq$ | $\supseteq$

Exercise.

NORMAL SUBGROUPS: REALITY

Wouldn't it be nice if $xHyH = \{xh_1yh_2 \mid h_1, h_2 \in H\}$ was actually the same set as $(xy)H$?

Not true for the subgroup $\{e, a\}$ of S_3 (check it).

$$(bH)(cH) = \{f, c, a, e\}.$$

Proposition (2.3.1)

Let H be a subgroup of G. If $gH = Hg$ for all $g \in G$, then

$$(xH)(yH) = (xy)H$$

for all x, y in G.

Proof: two inclusions. If $g \in (xy)H$ then $g = xyh = xeyh \in xHyH$. If $g \in xHyH$ then $g = xh_1yh_2$ for some $h_1, h_2 \in H$. Since $Hy = yH$ there exists h_3 so that $h_1y = yh_3$, so $g = xh_1yh_2 = xyh_3h_2 \in xyH$ since H is a subgroup. □

$\{gng^{-1} : n \in N\}$.

//

Definition (2.3.2)

A subgroup N is called *normal* if $gNg^{-1} = N$ for all $g \in G$.

or alternatively (Ex 2.11.13), $gN = Ng$ for all $g \in G$

Cor 2.3.3 → If H normal, G/H with multiplication $xH \circ yH = xyH$ forms a group.

Definition (2.3.4)

If N is normal in G, then the group G/N is called a *quotient group*.

Eg: $N = \{e, d, f\}$ of S_3 is normal (check this), so the group $S_3/N = \{N, aN\}$ is a group, and has order 2 (by Lagrange or just obvious). How many groups of order 2,3 are there?

$|S_3| = 6$, $|N| = 3$

$6 = 2 \cdot 3$

$[S_3 : N]$

I want to completely understand/classify ALL finite groups.

Write them all down in a nice list.

Here is my idea. Start with your finite group G. Does it have a (proper) normal subgroup? If yes, does that normal subgroup live inside a bigger one that is a proper normal subgroup as well? If so, pick a biggest one, N_1.

G/N_1

new group.

ANOTHER FANTASY IDEA

I want to completely understand/classify ALL finite groups.

Write them all down in a nice list.

Here is my idea. Start with your finite group G. Does it have a (proper) normal subgroup? If yes, does that normal subgroup live inside a bigger one that is a proper normal subgroup as well? If so, pick a biggest one, N_1.

Let $G_1 = G/N_1$. This is a smaller group (Lagrange).

Does G_1 have a normal subgroup? If yes, pick a biggest one and quotient it.

My "algorithm" will terminate because the groups are getting smaller each time. What does it terminate at?

ANOTHER FANTASY IDEA

I want to completely understand/classify ALL finite groups.

Write them all down in a nice list.

Here is my idea. Start with your finite group G. Does it have a (proper) normal subgroup? If yes, does that normal subgroup live inside a bigger one that is a proper normal subgroup as well? If so, pick a biggest one, N_1.

Let $G_1 = G/N_1$. This is a smaller group (Lagrange).

Does G_1 have a normal subgroup? If yes, pick a biggest one and quotient it.

My "algorithm" will terminate because the groups are getting smaller each time. What does it terminate at?

Definition (Simple)

If G has no proper normal subgroups (other that $\{e\}$ and G) then G is called *simple*.

How can I say one group is the same as another?

First we define a map which "preserves (group) structure"

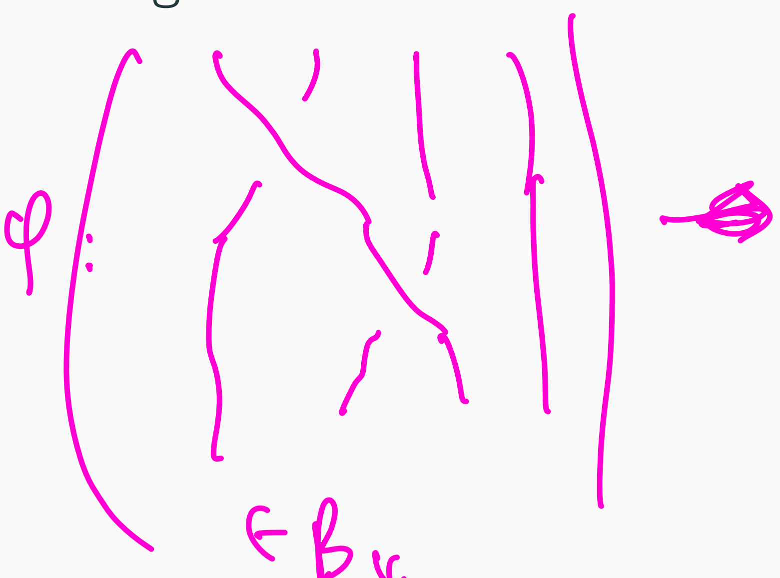
Definition (2.4.1)

Let G, K be groups. A map $f : G \to K$ is called a *group homomorphism* if $f(xy) = f(x)f(y)$ for all $x, y \in G$.

Eg: the map from $\mathcal{B}_4$ to S_4 which "forgets crossings" ← homom.

Eg: the determinant function from $GL(n, \mathbb{R})$ to $(\mathbb{R} \setminus \{0\}, \cdot)$

$\det : GL(n,\mathbb{R}) \to (\mathbb{R}\setminus\{0\}, \cdot)$



$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \in S_4$$

$$\det(AB) = \det(A)\det(B).$$

How can I say one group is the same as another?

First we define a map which "preserves (group) structure"

Definition (2.4.1)

Let G, K be groups. A map $f : G \to K$ is called a *group homomorphism* if $f(xy) = f(x)f(y)$ for all $x, y \in G$.

Eg: the map from $\mathcal{B}_4$ to S_4 which "forgets crossings"

Eg: the determinant function from $GL(n, \mathbb{R})$ to $(\mathbb{R} \setminus \{0\}, \cdot)$

Eg: any group G and the group $K = \{e\}$

How can I say one group is the same as another?

First we define a map which "preserves (group) structure"

Definition (2.4.1)

Let G, K be groups. A map $f : G \to K$ is called a *group homomorphism* if $f(xy) = f(x)f(y)$ for all $x, y \in G$.

Eg: the map from $\mathcal{B}_4$ to S_4 which "forgets crossings"

Eg: the determinant function from $GL(n, \mathbb{R})$ to $(\mathbb{R} \setminus \{0\}, \cdot)$

Eg: any group G and the group $K = \{e\}$

Eg: If N is a normal subgroup of G, then $\pi : G \to G/N$ defined by $\pi(g) = gN$ (ex: check)

~~Defn: homom, ker, epi, iso, isom theorem.~~

If $\varphi\colon G \to K$ is a homomorphism, define $\ker\varphi = \{g \in G \mid \varphi(g) = e_K\}$, called the *kernel* of φ.

Eg: What is the kernel of the homomorphism from $\mathcal{B}_4$ to S_4?

$\varphi: GL(n,\mathbb{R}) \to (\mathbb{R}\setminus\{0\}, \cdot)$

$\ker(\varphi) = \{A \in GL : \det(A) = 1\}.$

KERNEL

If $\varphi\colon G \to K$ is a homomorphism, define $\ker \varphi = \{g \in G \mid \varphi(g) = e_K\}$, called the *kernel* of φ.

Eg: What is the kernel of the homomorphism from $\mathcal{B}_4$ to S_4? Ans: the "pure braid group" (braids which preserve the order of the strands)

If $\varphi\colon G \to K$ is a homomorphism, define $\ker\varphi = \{g \in G \mid \varphi(g) = e_K\}$, called the *kernel* of φ.

Eg: What is the kernel of the homomorphism from $\mathcal{B}_4$ to S_4? Ans: the "pure braid group" (braids which preserve the order of the strands)

Eg: What is the kernel of the determinant map from $GL_n(\mathbb{R})$ to $(\mathbb{R} \setminus \{0\}, \cdot)$?

If $\varphi\colon G \to K$ is a homomorphism, define $\ker\varphi = \{g \in G \mid \varphi(g) = e_K\}$, called the *kernel* of φ.

Eg: What is the kernel of the homomorphism from $\mathcal{B}_4$ to S_4? Ans: the "pure braid group" (braids which preserve the order of the strands)

Eg: What is the kernel of the determinant map from $GL_n(\mathbb{R})$ to $(\mathbb{R} \setminus \{0\}, \cdot)$? Ans: $SL_2(\mathbb{R})$

Ex: If $\varphi: G \to K$ homom then $\varphi(e_G) = e_K$.

Proposition (part (ii) f 2.4.9)

If $\varphi: G \to K$ is a homomorphism, then $\ker(\varphi)$ is a normal subgroup of G.

subgroup.

Proof:

To ADD.

Proposition (part (ii) f 2.4.9)

If $\varphi\colon G \to K$ is a homomorphism, then $\ker(\varphi)$ is a normal subgroup of G.

Proof:

A kernel is a neat way to define new and interesting groups from exiting ones (eg. pure braid group, $SL_2(\mathbb{R})$, and the Alternating group coming up).

Proposition (part (iii) of 2.4.9)

Let $\varphi\colon G \to K$ *be a homomorphism.* $\ker(\varphi) = \{e\}$ *if and only if* φ *is injective (one-to-one).*

Proof:

IMAGE

Let $\varphi\colon G \to K$ be a homomorphism.

The *image* of φ is $\varphi(G) = \{\varphi(g) \mid g \in G\}$.

Claim: $\varphi(G)$ is a subgroup of K.

Proof:

A map $\varphi\colon G \to K$ is an *isomorphism* if it is

- a homomorphism
- a bijection

We say that G, K are *isomorphic* if there exists some isomorphism from one to the other. The is the notion of two groups being the same.

Eg All groups size 4

	e	a	b	c
e				
a				
b				
c				

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

two.

A map $\varphi \colon G \to K$ is an *isomorphism* if it is

- a homomorphism
- a bijection

We say that G, K are *isomorphic* if there exists some isomorphism from one to the other. The is the notion of two groups being the same.

Recall: finite group, multiplication table, what does an isomorphism do to the table?

ISOMORPHISM THEOREM (2.5.1)

Let G, K be groups and $\varphi\colon G \to K$ a group homomorphism with kernel $N = \ker(\varphi)$.

Then

$$\tilde{\varphi}\colon G/N \to \varphi(G)$$

defined by $\tilde{\varphi}(gN) = \varphi(g)$ is a well-defined map and a group isomorphism.

Proof: note the proof must first show the map makes sense (well defined) before proving properties about it. Well defined means: if I have two representatives of the same coset g_1N and g_2N, am I sure that the image of g_1 and g_2 will be the same?

Ex: do this proof (check Lauritzen after you attempt)

EG

Read Example 2.5.2 for an application of the isomorphism theorem (complex numbers).

Reading: we already discussed order of an element. Read 2.6, 2.7, 2.8 which defines "cyclic group", and links the abstract notions learned so far in Chapter 2 to number theory (Chapter 1).

Eg: Chinese remainder theorem is simply the fact that $n_1, \ldots, n_r$ pairwise relatively prime integers, then the map which sends n to its remainders mod $n_1, \ldots, n_r$ is a group isomorphism

$$\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

Next week:

- Permutation groups