<u>Definition</u>. Let G be a group and X a set. A (left) <u>group action</u> of G on X is a map

$$G \times X \longrightarrow X \qquad \text{(written } g \cdot x \text{ or } gx\text{)}$$

satisfying the following.

(1) $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$ for all $g_1, g_2 \in G$, $x \in X$

(2) $1 \cdot x = x$ for all $x \in X$.

<u>Examples</u>. (1) Let $G = \mathrm{Sym}(n)$ and $X = \{1, \dots, n\}$.

Then, for $\sigma \in G$, the map
$$G \times X \to X$$
$$(\sigma, x) \to \sigma(x)$$
defines an action.

(2) Let G be the image of D_n in $GL_2(\mathbb{R})$, as discussed before, and let

$$X = \{1, \zeta, \zeta^2, \zeta^3, \dots, \zeta^{n-1}\}$$
$$= \left\{(1,0), \left(\cos\tfrac{2\pi}{n}, \sin\tfrac{2\pi}{n}\right), \left(\cos\tfrac{4\pi}{n}, \sin\tfrac{4\pi}{n}\right), \dots, \left(\cos\tfrac{2\pi(n-1)}{n}, \sin\tfrac{2\pi(n-1)}{n}\right)\right\}$$

Then G acts on X. (Verify!)

(3) Vector spaces: Given V over a field F, the multiplicative group $F^\times$ acts on V.

(You can <u>multiply</u> elements of V by elements of F.)

Really you get a <u>module</u> for the <u>ring</u> F.

9.2.

(4) Let $\mathbb{H} = \{ z \in \mathbb{C} : \operatorname{Im}(z) > 0 \}$

(the "upper half plane").

Exercise: The group $SL_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_{2\times 2}(\mathbb{Z}) : \det = 1 \right\}$

acts by linear fractional transformations

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \circ z = \frac{az+b}{cz+d}.$$

What is to be checked?

(1) This does map $\mathbb{H} \to \mathbb{H}$.

(2) The "associative law".

(5) G acts on itself by left multiplication:

$$g \cdot h = gh.$$

(6) G acts on itself by conjugation.

$$g \cdot h = g h g^{-1}.$$ (The notation is confusing!)

(7) Let X = functions $\{1, \ldots, n\} \to \mathbb{C}$, $G = \mathrm{Sym}(n)$.

Exercise. ~~This map~~ Writing

$$(g \cdot f)(x) = f(gx)$$

does not, in general, define a group action of G on X.

But, writing

$$(g \cdot f)(x) = f(g^{-1}x)$$ does.

9.3.

(8) ~~An example similar to~~ [illegible]

Let V be a f.d. vector space.

Then $GL(V)$ acts on V by

$$\phi \cdot v = \phi(v).$$

(9.) Again, let V be a fd vector space,

let $V^* = \mathrm{Hom}(V, F)$ be its dual space.

Then $GL(V)$ acts on V. The map

$$(g \circ f)(v) = f(gv)$$

does <u>not</u> define a left group action.

But $(g \cdot f)(v) = f(g^{-1}v)$

and $(g \cdot f)(v) = f(g^T v)$ do.

~~Proposition~~

Note that an action of a group G on X gives an injective homomorphism

$$G \longrightarrow \mathrm{Sym}(X)$$

$$g \longrightarrow \pi_g = \{x \to gx\}.$$

Must prove:

(1) This defines a permutation (i.e. bijection) on X for each g, i.e. Really do get a map $G \to \mathrm{Sym}(X)$

(2) it's a group homomorphism.

9.4

(1) Show that π_g has a two-sided inverse, namely $\pi_{g^{-1}}$. For all x,

$$(\pi_{g^{-1}} \circ \pi_g)(x) = \pi_{g^{-1}}(\pi_g(x)) \quad \text{(def. of function composition)}$$
$$= g^{-1} \cdot (g \cdot x) \quad \text{(by def. of } \pi_g\text{)}$$
$$= (g^{-1} g) \cdot x \quad \text{(group action axiom)}$$
$$= 1 \cdot x$$
$$= x \quad (\text{" " "}).$$

Same for $\pi_g \circ \pi_{g^{-1}}$.

(2) Must prove: $\pi_{gh} = \pi_g \circ \pi_h$ as elements of $\mathrm{Sym}(X)$.

For all $g, h \in G$, $x \in X$,

$$\left.\begin{array}{l} \pi_{gh}(x) = (gh)(x) \\ \pi_g \circ \pi_h(x) = g(h(x)) \end{array}\right] \text{Same by group action axioms.}$$

Cayley's Theorem. Every group is isomorphic to a subgroup of ~~a~~ a symmetric group.

Proof. Saw earlier, G acts on itself by left multiplication, so the map

$$g \longrightarrow \pi_g = \{h \to gh\}$$

is a homomorphism $G \longrightarrow \mathrm{Sym}(G)$.

It is injective because if $h = gh$ for all $h \in G$, then $g = 1$.

(Indeed if $h = gh$ for any $h \in G$, then $g = 1$.)

9.5. ~10.11 Centralizers:

Definition. Let G be a group, with $A \subseteq G$ a subset. Then the centralizer of A is

$$C_G(A) = \{ g \in G : gag^{-1} = a \text{ for all } a \in A \}$$
$$= \{ g \in G : ga = ag \text{ for all } a \in A \}$$
$$= \{ \text{elts. of } G \text{ which commute with every element of } A \}.$$

If $A = \{a\}$ is a singleton, write $C_G(a)$.

Proposition. This is a subgroup of G (for arbitrary subsets A)

Prove it as an exercise.

The center of G, $Z(G)$ (auf Deutsch) $= C_G(G)$

$$= \{ g \in G : hg = gh \text{ for all } h \in G \}.$$

Note that $Z(G) = G \iff G$ is abelian.

Exercise. Find non-abelian examples of G for which $Z(G) = \{e\}$ and for which $Z(G) \supsetneq \{e\}$.

The normalizer of A is

$$N_G(A) = \{ g \in G : \underbrace{gAg^{-1}}_{\text{This is } \{gag^{-1} : a \in A\}} = A \}.$$

Conjugation preserves A as a set, not necessarily pointwise. So $C_G(A) \leq N_G(A)$.

Exercise. Come up with an example where these are different

10.2.

The stabilizer of a group action.

Def. Suppose a group G acts on X and $x \in X$.
The stabilizer of x in G is

$$G_x = \mathrm{Stab}_G(x) = \{ g \in G : g \cdot x = x \}.$$

The kernel of the action is

$$\bigcap_{x \in X} G_x = \{ g \in G : g \cdot x = x \text{ for all } x \in X \}.$$

Exercise. (1) These are subgroups.

(2) Recall the action of $G = SL_2(\mathbb{Z})$ on $\mathbb{H}$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \circ z = \frac{az + b}{cz + d}.$$

(a) What is the kernel of the action?

(b) Can you find a point in $\mathbb{H}$ with larger stabilizer?

(c) Can you find infinitely many?

Note that (b) $\to$ (c). Why?

Given your favorite z, then another element in the same orbit looks like γz for some $\gamma \in G$.

Now, if $gz = z$
then $g\gamma z$ may not be γz
But $(\gamma g \gamma^{-1}) \gamma z = gz$.

10.3. In other words.

Suppose G acts on a set X, and x_1 and x_2 are in the same orbit. This means $gx_1 = x_2$ for some $g \in G$.

(~~[illegible]~~ Check: this is an equivalence rel'n)

Then, $\mathrm{Stab}_G(x_1)$ and $\mathrm{Stab}_G(x_2)$ are conjugate;

$$\mathrm{Stab}_G(x_2) = g\, \mathrm{Stab}_G(x_1)\, g^{-1}.$$

(This is an equivalence relation too)

Example. (My favorite!)

Let $V = \{ au^3 + bu^2v + cuv^2 + dv^3 : a, b, c, d \in \mathbb{C} \}$

be the vector space of binary cubic forms.

(1) Prove that $G = GL_2(\mathbb{C})$ acts on V via

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \circ f(u, v) = f(\alpha u + \gamma v, \beta u + \delta v).$$

(2) The kernel of the action is cyclic of order 3.

(3) (Challenge!) If $f \in V$, then

$$\mathrm{Stab}_G(f) \begin{cases} \text{has size } 18 \text{ if } f \text{ doesn't have a repeated root} \\ \text{is infinite if it does.} \end{cases}$$

10.4. Definition. A group H is <u>cyclic</u> if it can be generated by a single element, i.e. if

$$H = \{ x^n : n \in \mathbb{Z} \} \quad \text{for some} \quad x \in H.$$

We call x a generator.
Note that x^{-1} is also a generator.

<u>Example</u>. Let

$$C_n = \langle x \mid x^n = 1 \rangle, \text{ the cyclic group of order } n.$$

Compute the orders of all elements of C_5 and C_6.
[Do at board]

If the group is abelian, we often write

$$H = \{ nx : n \in \mathbb{Z} \}.$$

<u>Example</u>. $\mathbb{Z}$ is also cyclic ("infinite cyclic") because 1 and only -1 are generators.

<u>Example</u>. S_n (for $n \geq 3$), D_n (for $n \geq 2$). <u>Not</u> cyclic.
Anything not abelian.

However, in any group G, ~~the~~ ~~for~~ each $g \in G$, the set

$$\langle g \rangle = \{ g^n : n \in \mathbb{Z} \} \quad \text{(subject to relations in } G\text{)}$$

<u>is</u> a cyclic subgroup.

10.5 $\equiv$ 11.1.

Some elementary propositions.

<u>Prop.</u> If $H = \langle x \rangle$, then $|H| = o(x)$, and:

(1) if $|H| = n < \infty$, then $x^n = 1$ and
$$H = \{1, x, x^2, \dots, x^{n-1}\}.$$

(2) If $|H| = \infty$, then $x^n \neq 1$ for $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b \in \mathbb{Z}$.

<u>Proof.</u> (1) The elements are distinct, because n is minimal such that $x^n = 1$ and $x^r = x^s \Rightarrow x^{r-s} = 1$.

Conversely, we've enumerated all of them:
An element in H looks like x^m for some $m \in \mathbb{Z}$.
Writing $m = qn + r$, with $0 \leq r < n$, $x^m = x^{qn+r} = (x^n)^q x^r = x^r$.

(2) is similar.

<u>Prop.</u> Let G be any group and $x \in G$, $m, n \in \mathbb{Z}$.

If $x^n = 1$ and $x^m = 1$ then $x^d = 1$ with $d := (m, n)$.

(2) If $x^m = 1$ for some $m \in \mathbb{Z}$, then $o(x) = |x|$ divides m.

<u>Proof.</u> (1) Use the <u>Euclidean</u> algorithm to write
$$d = mr + ns \quad \text{for some } r, s \in \mathbb{Z}.$$
Then $x^d = x^{mr+ns} = (x^m)^r (x^n)^s = 1$.

(2) $x^m = 1$ and $x^{o(x)} = 1$. Since $o(x)$ is <u>minimal</u>, $(o(x), m) = 1$ and $o(x) \mid m$.

11.2.

Some more boring propositions.

(1) Any two cyclic groups of the same order are isomorphic.

(2) A subgroup of a cyclic group is cyclic.

(3) You can compute the order of any elt. of a cyclic group.

We're more or less skipping the rest of Ch. 2.
But put the pretty pictures on the overhead.

Quotients.

Definition. If $X \xrightarrow{\varphi} Y$ is a map of $\{$sets, groups, ..., schemes$\}$, pretty much anything other than

then the fibers of φ are the sets

$$\{\varphi^{-1}(a)\} \text{ as } a \text{ ranges over } Y.$$

Example. Consider a surjective linear transformation $\mathbb{R}^3 \xrightarrow{\phi} \mathbb{R}^2$,

Its kernel will be a line.

What do the fibers look like?

Claim. $\phi^{-1}(w) = v + \mathrm{Ker}(\phi)$, where v is an arbitrary elt. of $\phi^{-1}(w)$, for each $w \in \mathbb{R}^2$.

Proof. If $v \in \phi^{-1}(w)$, then

$$v' \in \phi^{-1}(w) \iff \phi(v') = w = \phi(v) \iff \phi(v'-v) = 0$$
$$\iff v' - v \in \mathrm{Ker}(\phi).$$

11.3

In groups, as with vector spaces, the kernel of a homomorphism $G \xrightarrow{\phi} H$ is

$$\ker(\phi) = \{ g \in G : \phi(g) = 1 \}.$$

Then $\ker(\phi)$ and $\mathrm{Im}(\phi)$ are subgroups of G and H respectively. (See DF p. 75 for some basic properties.)

Proposition. Given $G \xrightarrow{\phi} H$ and let $K = \ker(\phi)$. Then, for any $h \in \mathrm{Im}(\phi)$, and any preimage $g \in \phi^{-1}(h)$,

$$\varphi^{-1}(h) = gK \quad \text{and}$$

$$\varphi^{-1}(h) = Kg.$$

Proof in both cases is the same!

Definition. A subgroup $N \leq G$ is normal if $gN = Ng$ for all $g \in G$. So, kernels of homomorphisms are normal.

Definition. If $N \leq G$ ~~are~~ is a subgroup, its

left cosets are $\{ gN : n \in N \}$

right cosets are $\{ Ng : n \in N \}$.

(If N is normal these coincide.) Note. All of them have size $|N|$.

Example. If $G = \mathbb{Z}$, $N = n\mathbb{Z}$, then the cosets are of the form $a + n\mathbb{Z}$ for $a \in \mathbb{Z}$. There are n of them.

Example. Let $G = D_n$. Then C_n is a normal subgroup. It has one coset.

11.4.

Example. The cosets of $SL_n(\mathbb{C})$ in $GL_n(\mathbb{C})$ are the sets of the form

$$\{ g \in GL_n(\mathbb{C}) : \det(g) = t \}$$

for each fixed $t \in GL_n(\mathbb{C})$.

~~Def~~ **Proposition.** Let N be a normal subgroup. Then the cosets of N in G form a group, with group operation

$$(Na)\cdot(Nb) = Nab.$$

This is called the quotient group of G by N and written G/N.

Proof. What's to prove? That it is well defined. If $Na = Nc$ and $Nb = Nd$, then $Nab = Ncd$.

~~The nicest way is to show that~~

If $Na = Nc$ then $a = n_1 c$ for some $n_1 \in N$, similarly $b = n_2 d$.

We have $Nab = Nn_1 c n_2 d$

$= Ncn_2 d$ ($Nn = N$ for any $n \in N$) (doesn't use normality)

$= cNn_2 d$ (normality)

$= cNd$ ~~(normal)~~ ($Nn = N$)

$= Ncd$ and we're done.

Alternative proof. Do it setwise,

$$Nab = \{ rs : r \in Na, s \in Nb \}.$$

More or less the same.

11.5

Example. $\mathbb{Z}/n\mathbb{Z} = \{\{a + n\mathbb{Z} : n \in \mathbb{Z}\} : a \in \mathbb{Z}\}$

$$= \{n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \dots (n-1) + n\mathbb{Z}\}.$$

$$(a + n\mathbb{Z}) \dot{+} (b + n\mathbb{Z}) = (a+b) + n\mathbb{Z}.$$

Example. Always have $G/G = 1$ and $G/1 \cong G$.

~~Example. There exists a surjective homomorphism $\mathrm{Sym}(n) \to \{\pm 1\}$ for every $n \geq 2$~~ True! But, on second thought, not relevant now.

Lagrange's Theorem. If H is a subgroup of the finite group G, then $|H| \mid |G|$.